



Title: Supply-chain and Trade Optimization based on Blockchain and Tokenization

Author: Silvan Andermatt

Affiliation: UZH

Date: 8.12.2021

1. Contents

1.	Contents	1
2.	Abstract.....	3
3.	Introduction	3
4.	What is DLT/ blockchain?.....	3
4.1.	Technology basics.....	3
4.2.	Consensus mechanics.....	4
4.2.1.	Proof of Work	4
4.2.2.	Proof of Stake	5
4.2.3.	Proof of Capacity	5
4.2.4.	Proof of Elapsed time	5
5.	What kind of blockchain exist?	5
5.1.	Public permissionless	5
5.2.	Public permissioned	5
5.3.	Private permissionless.....	6
5.4.	Private permissioned	6
6.	When to use a blockchain?	6
6.1.	Model of Wüst/Gervais.....	6
6.2.	Supply chain track-and-trace with Blockchain	7
7.	Why tokenisation of real world assets	7
7.1.	FINMA classification and DLT-securities token.....	7
7.2.	Token standards	9
7.2.1.	ERC-20	9
7.2.2.	ERC-721	9
7.2.3.	ERC-1155	10
7.2.4.	NEP-5	10
7.2.5.	BEP2.....	10
7.2.6.	Overview.....	10
7.3.	NFT vs FT	10
7.4.	Fragmentation	10
8.	Trading of token in the new world	11
9.	Where to trade?.....	11
9.1.	Comparison: Exchange, MTF, OTF, DLT-Exchange.....	11
9.2.	Stock Exchange.....	11
9.3.	Multilateral Trading Facility (MTF)	13
9.4.	Organised Trading Facility (OTF)	13
9.4.1.	Securities Firm.....	13
9.5.	DLT Trading Facility	15
9.5.1.	Regular DLT Trading Facility	15
9.5.2.	Small DLT Trading Facility	16
9.6.	Conclusion	16



10. References	17
11. Webreferences	21



2. Abstract

The paper introduces Blockchain technology and trading of options for token, applied on the use case of real world asset tokenization.

3. Introduction

The paper shall introduce general concepts of DLT / Blockchain and comparing existing solutions for the tokenization of real world assets, by analysing in particular the Swiss regulatory framework. Tokenization of real world assets becomes increasingly popular and the headlines in the press contribute to a potential hype for DLT / Blockchain technology, while at the same time an opposition is forming, claiming the non-sense of the same technology. By analysing the current state of technology and regulatory options we shall outline what are advantages and requirements of DLT / Blockchain for the use case of trading real world assets. The paper begins with an introduction to the technology and how it works. Then it offers an overview of the currently available Blockchains. Prior diving into the controverse question on when to use a Blockchain. It is then considered why tokenizing the real world and what would trading with the new assets require.

4. What is DLT/ blockchain?

4.1. Technology basics

Blockchains (BC) are part of Distributed Ledger (DL) systems, which are defined as a collection of independent computers that appear to its users as a single coherent system.ⁱ The system can be also described as network, whereby the single computers can be physically separated in a distributed or decentralized manner.ⁱⁱ As a consequence, there is concurrency among the connected computers, each of them could fail individually, without necessarily triggering major consequences for the resilience of the distributed system as a whole, so for instance in the case of the Internet.ⁱⁱⁱ

Distributed systems are perceived by the user as a single system and thus may conceal details on the single computer connected. It allows for a multitude of different computers to be connected, *e.g.*, all kind of laptops to the Internet, with different characteristics among them (*e.g.*, operating system, programming languages, technical specifications). The mechanics of failure handling may differ, *e.g.*, recovery procedures and redundancy handling can vary across different distributed systems. Oftentimes, distributed systems are characterized by facilitating its extension to include *e.g.*, further computers to the internet.^{iv} With this openness to include more participants comes the need to handle scalability, which include handling costs of resources to operate a growing network while still optimizing its performance. With the growing number of computers connected to a network, security concerns may arise concerning how to keep data secrecy, privacy and integrity, as well as how to setup the authentication and authorization of users, *i.e.*, there is a trade-off between security and functionality, because the most secure solution is likely the most cumbersome for users (*e.g.*, multi factor authentication), while the most comfortable may bear the highest security risks for the network (*e.g.*, single factor or no-authentication).^v

The Internet has then been used as a base layer for further technology developments, such as BCBC, an overlay network. An overlay network is built on top of an underlay network, *i.e.*, BC is a overlay network on the Internet as underlying network, and the two networks are connected virtually or logically.

A Peer-to-Peer (P2P) system is „a self-organizing system of equal [which] equal, autonomous entities (peers) aims for the shared usage of distributed resources in a networked environment avoiding central



services“.^{vi} Therefore, all peers are in principle equal, share resources provided by other peers and communicate directly and without intermediaries with other peers, furthermore, the network is decentralized and coordinates itself from within.^{vii}

4.2. Consensus mechanics

BC is a trustless. Peers do not need to trust each other in a BC environment, they only trust the system. In such an environment it is of essence to define how an additional block is added and accepted by the BC. Here fore, several consensus mechanisms have been developed over time.

4.2.1. Proof of Work

The Proof of Work (PoW) is a consensus mechanism, where in order to add a new block to the BC a mathematical puzzle must be solved.^{viii} The correct solution is a hash value with a number of zeros in the beginning, which is easy to verify albeit difficult to produce. The number of initial zeros is constantly adjusted to amend the difficulty of the mathematical puzzle, depending on the computing power of the involved nodes (so called miners) for the previous block, so to meet a target of *e.g.*, adding in average a new block to the bitcoin BC every 10 minutes.

A hash is the output of a cryptographic function, such as SHA-256. It has always the same length (fixed integer size), so that regardless of the size of the input (*e.g.*, a single character or a whole book), the output will always be the same and predefined amount of numbers and characters. Therefore, it is not possible to establish the size of the input data based on the hash. Furthermore, the hash change completely with only the slightest amendment of the input data. However, as long as the input data is exactly the same, the output will also always be the same (deterministic). Thus, basically everyone can validate a hash, knowing the input, but it is virtually impossible to guess the input by only having the hash (reverse engineer).

BC leverage the above properties of the hash to secure the history of the data. Every block is hashed and this hash is included in the following block. Due to the properties of hash to change massively with an amended input, any change to the previous block would result in an amended hash of that block, and in consequence also of the hash of any following block. Therefore, tempering a block of the BC would result in all the subsequent blocks being different and may eventually be rejected by the consensus mechanism of the BC. Henceforth, a PoW-based BC becomes tamper proof.

In order to find a target hash, the input must amended until the output matches the defined criteria. This is done by including a random number only used once (nonce) with the input data. Since the nonce is constantly changing, the output will as well, offering a mathematical puzzle that can be solved with trials but not logic (brute force). To find the correct hash as early as possible, significant resources must be invested, depending on the size of the network. In the case of Bitcoin it is difficult for a node operated on a laptop to first find the correct hash, since there are nodes with specialized hardware and much higher hash computing power (hash rate)^{ix}. Since the competition is high, dedicated groups of collaborating miners were founded (mining pools).^x Mining pools share the nonce values for a same data (previous block hash plus the transactions to be included in the current block) among the participants in the pool, so that every participants ends up only using certain nonce, but avoiding to use the same nonce among two or more participants within the mining pool, resulting in increased efficiency and thus higher chances to obtain rewards.

In order to incentivize miners to dedicate computing power to the network, and therefore, investing considerable resources into securing the network, maintenance of the hardware and not negligible energy consumption, the first miner validating a new block is granted a reward.^{xi} The reward may consist of



block reward (to mine a block) and of transaction fees (to include transaction data in a mined block), paid in a cryptocurrency.

The block reward is generally predefined at creation of a BC to increase early adoption of the BC. In the beginning of a BC lifespan there are only few or no transactions on the BC and therewith also very little transaction fees to be earned by validating blocks. However, a BC needs miners in order to operate, so offering a higher block reward in the beginning has proven successful. Over time the BC will attract more participants, generating more transactions, thus diminishing the need for block rewards. In fact, oftentimes there is a mechanism reducing the block reward every certain amount of blocks (halving).

The transaction fees on the other side, may remain constant over time, *e.g.*, based on the amount of data included in a block (number of transactions). However, due to the likely increasing value of the cryptocurrency earned for mining a block, even though the relative amount is unchanged, in absolute terms the miner is earning more than in the early days of the same BC. The gradual shift from block reward to transaction fees should guarantee sufficient incentives for nodes to mine blocks over the whole lifetime of a BC.

4.2.2. Proof of Stake

The Proof of Stake (PoS) is a consensus mechanism based on the concept that miner with a higher number of token or coins at stake shall be granted a respectively directly proportionally higher amount of mining power, therewith more likely obtaining a reward. PoS was intended to solve the energy consumption issue arising from using PoW. Among the backdrops is that a pure PoS approach bears inherent incentives for misuse, since miners with the biggest stake could leverage their position to benefit from misconduct (such as falsely granting themselves higher token balances). A possible solution is that miners involved into misconduct loose the stake if ascertained (slashing).^{xii}

4.2.3. Proof of Capacity

The Proof of Capacity (PoC) is a consensus mechanism based on allowing miners with sufficient storage capacity to mine blocks, in the sense that miners are staking their storage capacity (analogous the PoS).

4.2.4. Proof of Elapsed time

The Proof of Elapsed Time (PoET) is a consensus mechanism based on equally distributing the chances to mine a block amongst all nodes in the network by establishing a random waiting time prior creating a new block for each node in the network, putting nodes in a sleep mode until its turn comes up.

5. What kind of blockchain exist?

5.1. Public permissionless

In public permissionless BCs everyone can read data from and write data on the BC. Further, is everyone allowed to participate in consensus mechanism. Resulting overall in full transparency without restrictions. This kind of BC is often considered the “true BC” or just “public BC”.

5.2. Public permissioned

In public permissioned BCs writing data on the BC as well as participating in the consensus mechanism is restricted, while reading data from the BC is open to everyone. This are used for collaborative environments that need a certain amount of control regarding data contributed to the BC and its reliability.



5.3. Private permissionless

In private permissionless BC writing data on the BC as well as participating in the consensus mechanism is restricted to specific participants. Reading data from the BC is partially open. This is often seen where a group of participants intend to collaborate, excluding others, but may disclose part of the information on the BC.

5.4. Private permissioned

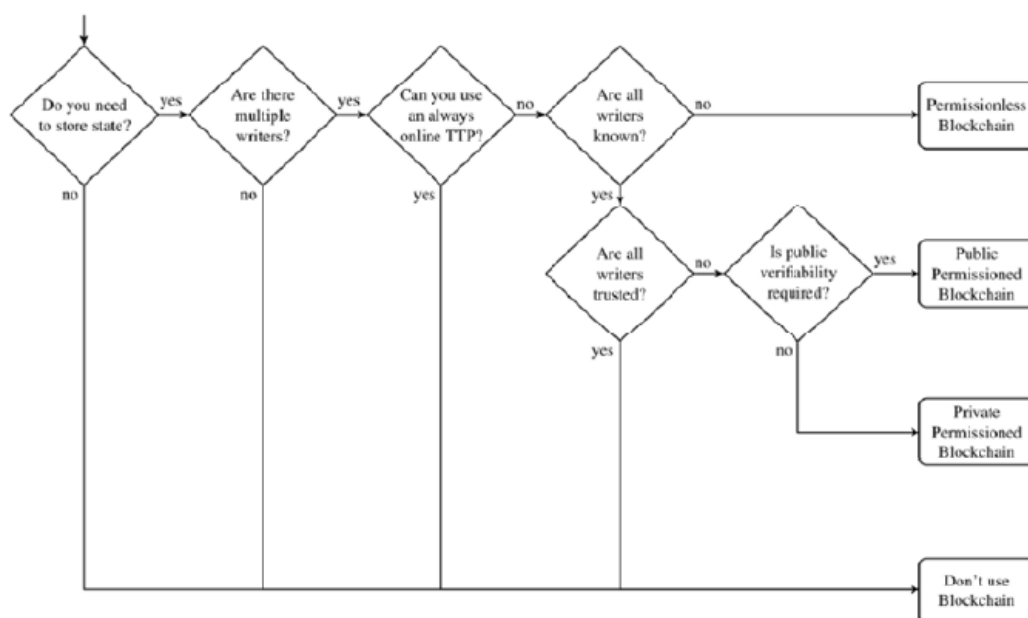
In private permissionless BC all elements are restricted to authorized participants, *i.e.*, reading data from, writing data on the BC as well as contributing to the consensus mechanism. This is used mostly within a single company, with full control over who is contributing data to the BC, reading out information and validating new blocks.

6. When to use a blockchain?

BC was first known in the context of Bitcoin and cryptocurrencies, becoming then increasingly popular with smart contracts and decentralised finance (DeFi), as well as with the ever-rising amount of total value locked in BC related projects.^{xiii} With the headlines and media coverage BC was also blamed for shifting towards a hype and being used for projects not actually benefitting from the technology.

6.1. Model of Wüst/Gervais

In order to determine if a BC is needed Wüst/Gervais established a decision tree model based on a specific set of questions.



K. Wüst, A. Gervais, 2017

The proposed model suggests that as long as there is no need to store a state, or there is only one writer, or a trusted third party (TTP) that is always online can be used, or all writers are known and trusted, there is no need for a BC. This leaves the use of BC for setups in which there is need to store a state and there is not an always available TTP, further, there are multiple writers. If all writers are known, a permissioned BC would be suitable, if not all writers are known and trusted, then depending on the requirements on public verifiability, either a public permissioned BC (public verifiability required) or private permissionless BC (public verifiability required) is most suitable.



6.2. Supply chain track-and-trace with Blockchain

For the use case of tracking and tracing material along a supply chain we can apply the model as follows. Firstly, we need to store in the BC the current status of the material (*e.g.*, stored in lots at warehouse based in Rotterdam) in the BC (store state). Secondly, in the course of a typical supply chain multiple participants are involved, from producer, to refinery, shipping, storage and sales, participants should be able to write on the BC, therefore multiple writers are involved. Thirdly, an always online TTP may be available, however if this is not the case, then a BC would be a better option, and since supply chains may range over the whole world with potentially unstable internet connection, the safer assumption is to use a BC. At this stage it comes down to design choices for the most suitable type of BC. While it may be possible to depict scenarios with unknown participants in a supply chain it is rather likely that participants are known to each other. However, this does not mean that participants are trusted, leaving two final options. Either the status on the BC needs to be publicly verifiable (public permissioned BC) or the not (private permissioned BC). A company regularly needs to disclose information to auditors and authorities, known third parties, but not to a general public, therefore the private permissioned BC, such as IBM Hyperledger, is likely the best solution.

Due to developments of privacy mechanisms on public permissionless BCs, they became a viable option. In fact, Zero Knowledge Proofs (ZKP) allows one party (prover) to prove to the other party (verifier), that they know a common secret, while not disclosing anything more than this to the other party^{xiv}. This can be used to confirm a transaction, while concealing information about the sender, receiver and further transaction details.

7. Why tokenisation of real world assets

7.1. FINMA classification and DLT-securities token

The Swiss Financial Market Authority FINMA recognised the innovation potential of distributed ledger technology (DLT) and BC technology when publishing guidance on the regulatory treatment of initial coin offerings (ICO) on 29th September 2017.^{xv} In the mid of a raising number of ICOs regulatory guidance was sought after by many, and FINMA was likely the world's first regulator offering it, since there was neither a global nor a Swiss regulatory framework for ICOs and in general for Token generating events (TGE).

FINMA welcomed and supported “all efforts to develop and implement BC solutions in the Swiss financial centre”.^{xvi} Instead of issuing completely new regulations, the initial guidance for ICOs followed a proven approach for financial markets legislation, it was principle based, *e.g.*, substance over form, same risks - same rules and technology neutral. Therefore, already existing laws and regulations were applied where suitable. Anty money laundering (AML) provisions were applied where the creation of a token by an ICO vendor involves issuing a payment instrument. Banking laws are applied when public deposits were accepted, if no exception was applicable. Dedicated laws were applicable for token qualifying as securities or in cases where assets were collected and managed externally. On the other hand, FINMA considered unregulated collecting funds for the own account, without intermediary, obligation of repayment, issuance of a payment instrument or offering of secondary market. Overall, FINMA analysed closely the developments and initiating enforcement procedures,^{xvii} in numerous cases where it was deemed necessary due to breach or circumvention of financial market legislation. ICO organizing parties were welcomed to share queries with the in 2016 newly operational FinTech desk.^{xviii}

After five months of publishing the FINMA guidance regarding ICOs, the most extensive FINMA Guidelines for enquiring regarding the regulatory framework for ICOs were issued.^{xix} The purpose of



the new guidelines is supporting market participants with information about how FINMA processes enquires for ICO and the principles according to which FINMA would react. For instance, minimum information requirements for ICOs were published.^{xx} However, the most important addition was a token categorization. FINMA defined three main categories of token (payment token, utility token, asset token) and a hybrid token category, for token including elements from more than one basic token category.

The FINMA classification can be simplified as follows

Token	Description	Treatment
Payment token	Synonymous with cryptocurrencies and defined as tokens which are intended to be used, now or in the future, as a means of payment for acquiring goods or services or as a means of money or value transfer. Cryptocurrencies give rise to no claims on their issuer	Not treated as securities, <i>e.g.</i> , Bitcoin and Ether.
Utility tokens	Tokens which are intended to provide access digitally to an application or service by means of a BC-based infrastructure	Not treated as securities if their sole purpose is to confer digital access rights to an application or service and if it can actually be used in this way at the point of issue, since the underlying function to grant access rights and the connection with capital markets, is missing
Asset tokens	Represent assets such as a debt or equity claim on the issuer. Asset tokens promise, for example, a share in future company earnings or future capital flows. In terms of their economic function, therefore, these tokens are analogous to equities, bonds or derivatives. Tokens which enable physical assets to be traded on the BC also fall into this category	Considered as securities (Article 2 let. b FMIA), if they represent an uncertificated security or a derivative (<i>i.e.</i> , the value of the conferred claim depends on an underlying asset), and the tokens are standardised as well as suitable for mass standardised trading,
Hybrid tokens	Outcome of the fact that the individual token classifications are not mutually exclusive, therefore allowing a token to present characteristics of more than one basic category, resulting in cumulative application of requirements for each of the contained category of token	



Figure 1 - FINMA token classification

In the second half of 2018 FINMA counted an increasing number of ICO project applications of tokens known as “stable coins”. These projects frequently aimed at overcoming the volatility of cryptocurrencies, one of their primary shortcomings, allowing for higher market acceptance. This was often links (*i.e.*, pegs) the value of the token to underlying assets, such as for instance a single fiat currency or a basket of fiat currencies.^{xxi} Unfortunately, stable coin arrangements were not always as stable as the public was meant to believe.

Stablecoins can be found in various designs, varying from a technical, legal, functional and economical perspective. Overall three categories can be observed: 1) Stablecoins with real world assets as underlying (*e.g.*, commodities). 2) Stablecoins with digital asset underlyings (*e.g.*, a basket of cryptocurrencies). 3) Stablecoins based on algorithmic price stabilizing mechanisms without any underlying.^{xxii}

FINMA offered detailed guidance on selected use cases. Stablecoins linked to fiat currencies with a fixed redemption claim and the underlying assets are managed for the account and the complete risk (*e.g.*, losses, from interest, fluctuations in the value of financial instruments, counterparty or operational risks) of the issuer, would usually result in the acceptance of deposits under the banking law, while if the redemption claim is dependent on future price developments and the underlying assets are managed for the account and risk of the token holder, it may fall under the CISA.

FINMA regularly found stablecoin projects bearing potential licensing requirements under the Banking Act (BA)^{xxiii} or the Collective Investment Schemes Act (CISA)^{xxiv}. If deemed a payment system of significant importance, a licensing requirement under the Financial Market Infrastructure Act (FMIA)^{xxv}. Usually, at least the Anti-Money Laundering Act (AMLA)^{xxvi} is deemed applicable, due to the purpose as a means of payment.

7.2. Token standards

As a result of the increasing adoption and utilization of token, standards were developed, since a standard interface allows tokens on Ethereum (ETH) to be re-used by third-party applications (*e.g.* wallets, decentralized exchanges).^{xxvii} Especially in the public permissionless blockchains, three main token types were observed.

7.2.1. ERC-20

The ERC-20 (Ethereum Request for Comments 20), has been proposed by Fabian Vogelsteller in November 2015. It implements an API for tokens within smart contracts and is likely the most common standard for cryptocurrencies as of today on ETH.^{xxviii} In fact, there are websites offering the creation of ERC 20 tokens for free in less than one minute.^{xxix} ERC-20 standard provides basic functionality for transferring tokens and allows tokens to be approved to be spent by another on-chain third part.^{xxx} The basic functionalities also allow to get the current token balance of an account and the total supply of the token available on the network.^{xxxi} ERC 777 is backwards compatible to ERC 20, but is further developed and allows additional use cases.^{xxxii} ERC 20 and ERC 777 are fungible tokens.

7.2.2. ERC-721

The ERC-721 (Ethereum Request for Comments 721), was proposed by William Entriken, Dieter Shirley, Jacob Evans, Nastassia Sachs in January 2018, based on two years of learning with ERC-20 to better support tracking of non-fungible tokens.^{xxxiii} ERC-721 provides functionalities like transferring tokens from one account to another, to get the current token balance of an account and the owner of a specific token as well as the total supply of the token available on the network. Further it can be approved



that an amount of token from an account can be moved by a third party account.^{xxxiv} Examples of ERC-721 include collectibles such as CryptoKitties and CryptoPunks.^{xxxv}

7.2.3. ERC-1155

The ERC-1155 (Ethereum Request for Comments 1155), was proposed by Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford in June 2018. The proposal is based on the recognition that existing token standards as ERC-20 and ERC-721 require a separate contract to be deployed for each token type or collection, placing a lot of redundant bytecode on the Ethereum blockchain and limiting certain functionality by the nature of separating each token contract into its own permissioned address. In this regard the ERC-1155 is a standard interface for contracts that manage multiple token types.^{xxxvi} The ERC-1155 token can do the same functions as an ERC-20 and ERC-721 token, and even both at the same time, but also improve the functionality of both standards, with efficiency gains, while correcting implementation errors on the ERC-20 and ERC-721 standards.^{xxxvii} ERC-1155 allows for transferring multiple token types at once, saving on transaction costs, e.g. trading (escrow / atomic swaps) of multiple tokens can be built on top of ERC-1155 and removing the need to “approve” individual token contracts separately.^{xxxviii} Examples are Enjin.^{xxxix}

7.2.4. NEP-5

NEP-5 is the technical standard used to implement and launch tokens on the NEO blockchain.^{xi}

7.2.5. BEP2

The BEP 2 standard is a technical standard used to implement and launch tokens on the Binance blockchain.^{xli}

7.2.6. Overview

The above tokens standards can be simplified and depicted as follows:

Token standard	ERC-20	ERC-721	ERC-1155
Blockchain	Ethereum	Ethereum	Ethereum
FT / NFT	FT	NFT	Both
Transfer	Yes	Yes	Yes

7.3. NFT vs FT

Token standards can be distinguished as fungible and non-fungible, with some further semi-fungible options.^{xlii} Fungible tokens (FT), described as tokens that are interchangeable among them, i.e. like fiat money, where a five euro bill equals another five euro bill.^{xliii} Non-fungible tokens (NFT), the opposite of FT.^{xliv}

7.4. Fragmentation

A token can be fragmented facilitating the trade of very tiny fraction of a token. As a reference, one bitcoin is splitted into 100 million smaller parts, called Satoshi. While buying a bitcoin comes at a price tag of around USD 62'000, small investors can buy a Satoshi for USD 0.0006. Therefore, even if the price of one Bitcoin would increase by a 100 times the current market value, then one Satoshi would cost around the smallest CHF fiat coin available (5 cents).



8. Trading of token in the new world

Blockchain is an immutable record of all transactions ever performed on the blockchain.^{xliv} The record, depending on the type of Blockchain, may be accessed by all or selected participants.^{xlvi} This allows for enhanced transparency, e.g. trade discovery, in relation to current status and access to the database^{xlvii}. Digitizing paperwork, by e.g. including information during the tokenization process, it can be avoided to share, check and amend the documents along a supply chain or trading partner chain, resulting in potential for significant efficiency gains^{xlviii}. Fragmentation of token may also support lower entry barriers for investors, thus boosting accessibility.^{xlix} Further, with the atomic swap, counterparty risks are reduced and the settlement is almost immediate, as opposed to T+2 in the old world.¹

9. Where to trade?

9.1. Comparison: Exchange, MTF, OTF, DLT-Exchange

The Swiss regulatory framework foresees a defined number of licensed forms of trading facilities. The most traditional is the stock exchange (Exchange), then there are Multilateral trading facility (MTF) and organized trading facility (OTF), as well as the DLT-Exchange. If a trading facility allows for trading of a token depends on the trading facility but also on the product (token), i.e. on its classification according to the financial markets regulation.

9.2. Stock Exchange

An exchange is an institution for multilateral securities trading where securities are listed, whose purpose is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules (Art. 26 lit. b FMIA).

The Exchange is supervised by FINMA, but can establish its own regulatory and supervisory organisation in line with its activities, with FINMA approving the directors appointed for this tasks and the regulations (Art. 27 para. 1, 3 and 4 FMIA). Furthermore, independence must be guaranteed between the regulatory and supervisory body, in addition to providing the guarantee of irreproachable business conduct, enjoying a good reputation, and having the specialist qualifications required for their functions (Art. 27 para. 2 FMIA).

The Exchange needs to issue regulations for orderly and transparent trading, in particular to register all of its orders and transactions in chronological order, as well as the transactions reported to it, by indicating the time, the identity of the participants, the securities traded and their number or nominal value, as well as their price (Art. 28 FMIA).

The Exchange shall publish the bid and offer prices for shares and other securities in real time, as well as the sizes of the trading positions at these prices (pre-trading transparency). Also the Exchange must immediately publish information on the transactions carried out on the trading venue and on the transactions conducted outside of the trading venue reported to it for all securities admitted to trading (post-trading transparency), This implies in particular the publication of the price, volume and time of the transactions (Art. 29 FMIA).

A trading venue which operates a technical platform must have a trading facility that guarantees orderly trading even in the event of intense trading activity, with effective measures preventing disruption (Art. 30 FMIA). When a decision is taken to suspend trading in a security listed on it at the initiative of the issuer or due to extraordinary circumstances, the Exchange shall immediately publish its decision, and it shall also be suspended on all of the other trading venues where the security in question is admitted to trading (Art. 33 FMIA).



The Exchange shall supervise price formation and the transactions conducted on the trading venue so that insider trading, price and market manipulation and other violations of statutory and regulatory provisions can be detected, also on transactions conducted outside of the trading venue that are reported to it or are brought to its attention in any other way (Art. 31 para 1 FMIA). In the event of suspected violations of the law or other irregularities, the body responsible for supervising trading (trading supervisory body) shall notify FINMA, in case of criminal offences, it shall also inform the competent prosecution authority without delay (Art. 31 para 2 FMIA).

The Exchange shall issue regulations on the admission, duties and exclusion of participants, thereby observing in particular the principle of equal treatment, albeit only the following can be admitted: a) securities firms in accordance with Article 2 letter d of the Financial Institutions Act of 15 June 2018¹⁷ (FinIA), b) other parties supervised by FINMA in accordance with Article 3 of the Financial Market Supervision Act of 22 June 2007¹⁸ (FINMASA), provided that the trading venue ensures that they fulfil equivalent technical and operational conditions to securities firms; c) foreign participants authorised by FINMA in accordance with Article 40, d) the Swiss National Bank (SNB) (Art. 34 FMIA).

The Exchange shall issue regulations on the admission of securities to trading, and particularly for the listing of securities and shall monitor compliance with the regulations as well as impose the sanctions provided for contractually in the event of violations (Art. 35 para 1 and 3 FMIA). The regulations of the Exchange shall take account of recognised international standards and in particular shall contain provisions on: a) the requirements that apply to the securities and the issuers and the duties of the issuer, its representatives and third parties in connection with the listing or admission of securities to trading; b) the publication of information on which investors rely for assessing the characteristics of securities and the quality of the issuer; c) the duties of the issuer, its representatives and third parties for the entire duration of the listing or admission of securities to trading; d) the obligation, regarding the admission of equity securities and bonds, to comply with Articles 7 and 821 of the Federal Act of 16 December 2005 on the Licensing and Oversight of Auditors (AOA) (Art. 35 para 2 FMIA).

The Exchange needs to appoint an independent appeal body to which application may be made: a) when a participant is refused admission; b) when a security is refused admission; c) when a participant is excluded; d) when a security is delisted (Art. 37 para 1 FMIA). While the Exchange shall govern the organisation of the appeal body and its procedures, FINMA has to approve the organisation, the procedural rules and the appointment of the members of the appeal body (Art. 37 para 2 and 3 FMIA).

Participants admitted to an Exchange shall keep a record of the orders and transactions they carry out, providing all the details necessary for overseeing and supervising their activity (Art. 38 FMIA).

The participants admitted to a trading venue must report all of the information necessary for transparent securities trading, exception made for SNB, according to the requirements of FINMA in regard of which information is to be reported to whom and in what form (Art. 39 FMIA).

If a foreign participant with no office in Switzerland wishes participating on a Swiss Exchange, FINMA shall grant authorisation: a) if it is subject to appropriate regulation and supervision; b) if it observes a code of conduct and record-keeping and reporting duties equivalent to the duties set out in Swiss regulations; c) if it ensures that its activities are separate from the activities of any authorised Swiss units; and d) if the competent supervisory authorities do not have any objections to the participant's activity in Switzerland and provide FINMA with administrative assistance (Art. 40 FMIA). However, FINMA may also reject authorisation if the state in which the foreign participant has its registered office does not grant Swiss participants actual access to its markets or does not offer them the same competitive opportunities as those granted to domestic trading participants (Art. 40 para 2 FMIA). For foreign



participants that are already admitted to participating in a Swiss trading venue facilitations apply, i.e. FINMA shall be informed if about the wish to participate in another Swiss trading venue and the foreign supervisory authority has to confirm that it has no objection to the expansion of the foreign participant's activity in Switzerland (Art. 40 para 3 FMIA).

9.3. Multilateral Trading Facility (MTF)

An MTF is an institution for multilateral securities trading whose purpose is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules without listing securities (Art. 26 lit. c FMIA).

The MTF shall issue regulations on the admission of securities to trading, particularly setting out the requirements for the securities and the issuers or third parties in connection with admission to trading, and monitor compliance with the regulations and impose the sanctions provided for contractually in the event of violations (Art. 36 FMIA).

For the reminder, the same rules as for the Exchange apply (Art. 26 lit. a FMIA).

9.4. Organised Trading Facility (OTF)

An OTF comes into three options: a) multilateral trading in securities or other financial instruments whose purpose is the exchange of bids and the conclusion of contracts based on discretionary rules; b) multilateral trading in financial instruments other than securities whose purpose is the exchange of bids and the conclusion of contracts based on non-discretionary rules; c) bilateral trading in securities or other financial instruments whose purpose is the exchange of bids (Art. 42 FMIA).

An OTF is subject to authorisation as a bank (Art. 1 BankA), securities firm ([Art. 41 FinIA](#)) or DLT trading facility, or authorisation or recognition as a trading venue (Exchange or MTF) to being operated (Art. 43 para 1 FMIA). Exception is made for intragroup setups, i.e. within a financial group if this is conducted via a legal entity that: a) is controlled directly by a financial market infrastructure; and b) is subject to consolidated FINMA supervision (Art. 43 FMIA).

9.4.1. Securities Firm

Securities firm is an entity that, on a commercial basis (i.e. if they directly or indirectly manage accounts or hold securities in safekeeping for more than 20 clients)^{li}: a) trades in securities in its own name for the account of clients; b) trades in securities for its own account on a short-term basis, operates primarily on the financial market and could thereby jeopardise the proper functioning of the financial market (if the total volume of executed trades in securities exceeds CHF 5 billion per calendar year in Switzerland)^{lii}, or is a member of a trading venue, or operates an organised trading facility under Article 42 of the Financial Market Infrastructure Act of 19 June 2015; or trades in securities for its own account on a short-term basis and publicly quotes prices for individual securities upon request or on an ongoing basis (market maker) (Art. 41 FinIA). It is required having its registered office in Switzerland and have the legal form of a commercial enterprise (Art. 42 FinIA). In the event of being foreign-controlled, the provisions for banks apply per analogy (Art. 43 FinIA). The securities firms must be able to be represented by a person who has their place of residence in Switzerland and is member of the body responsible for its management (at least two people) or (in particular for Firms trading for the account of clients and firms acting as market makers) of the body responsible for its governance, supervision and control (Art. 66 para 1-3 FinIO). Securities firms must have an appropriately defined risk management system in place as well as an effective internal control structure, and keep functions separated (Art. 68 para 1 and 3 FinIO). Provided legitimate grounds, FINMA may allow relaxations of



these requirements or it may impose more stringent requirements (Art. 66 para 4 and Art. 68 para. 5 FinIO).

In particular, the securities firm may: a) hold accounts for settling securities trade within the context of its activity under Article 41 for clients, either itself or with third parties, accepting deposits from the public on a commercial basis within the context of its activity;^{liii} b) act as custodian of clients' securities, either itself or in its own name with third parties; c) underwrite securities issued by third parties as a firm commitment or on commission and offer these to the public on the primary market on a commercial basis; d) create derivatives itself on a commercial basis, which it offers to the public on the primary market on its own behalf or that of another party (Art. 44 FinIA).

Securities firms trading for the account of clients or acting as market makers within the meaning of Article 41 letters a and c FinIA shall appoint internal auditors, which are independent of management, provided with sufficient resources as well as unlimited audit rights (Art. 68 para. 4 FinIO).

Securities firms must possess the required minimum capital fully paid up, however, FINMA may permit securities firms in the form of partnerships to post appropriate collateral instead of the minimum capital (Art. 45 FinIA). The minimum capital is at least CHF 1.5 Mio, paid up in full and maintained at all times (Art. 69 para 1 FinIO).

Securities firms must have sufficient own funds and liquidity individually and on a consolidated basis, diversifying their risks appropriately according to the requirements of the Federal Council (Art. 46 para 1-3 FinIA). FINMA may ease the requirements or order more stringent requirements, where there are legitimate grounds for so doing, (Art. 46 para 4 FinIA). Additional capital and Accounting requirements apply in analogy to the requirements set forth in the BankA (Art. 47 f. FinIA).

Two or more companies are deemed to be a financial group dominated by a securities firm if: a) at least one of them operates as a securities firm; b) they operate primarily in the financial sector; and c) they form an economic unit or other circumstances suggest that one or more of the companies under individual supervision is de jure or de facto obliged to provide assistance to group companies (Art. 49 para 1 FinIA). A financial conglomerate dominated by a securities firm is a financial group as defined in paragraph 1 operating primarily in the field of securities trading and comprising at least one insurance company of considerable economic significance (Art. 49 para 2 FinIA). The provisions of the BankA on financial groups and financial conglomerates apply by analogy (Art. 49 para 3 FinIA).

The securities firm must keep a record of the orders and transactions it conducts together with all the details necessary for their traceability and for the supervision of its activity (Art. 50 FinIA).

The securities firm must report all of the information necessary for transparent securities trading and FINMA shall regulate which information is to be reported to whom and in what form (Art. 51 para 1 and 2 FinIA). Provided this is required for the purposes of the Act, the Federal Council may also impose the reporting duty in accordance with paragraph 1 on persons and companies that buy and sell securities on a commercial basis but without the involvement of a securities firm. Any such company must instruct an audit firm licensed by the Federal Audit Oversight Authority (FAOA) in accordance with Article 9a paragraph 1 of the Auditor Oversight Act of 16 December 2005²⁴ (AOA) to audit compliance with this reporting duty and must inform FINMA (Art. 51 para 3 FinIA).

An OTF operator must: a) do this separately from the other business activities; b) take effective organisational measures to identify, prevent, settle and monitor conflicts of interest; c) ensure that client interests are comprehensively protected when conducting proprietary transactions on the organised trading facility operated by him (Art. 44 FMIA).^{liv}



An OTF operator must ensure that this guarantees orderly trading even in the event of intense trading activity and shall take effective measures to prevent disruptions to the trading facility (Art. 45 FMIA).^{lv}

An OTF operator shall publish information on the transactions carried out on the trading facility, in particular the price, volume and time of the transactions, taking recognised international standards and foreign legal developments into account, in line with the exemptions to this publication duty as defined by the Federal Council, particularly in relation to securities transactions involving large volumes or that are executed by the SNB.^{lvi}

9.5. DLT Trading Facility

9.5.1. Regular DLT Trading Facility

A DLT trading facility is a commercially operated institution (independent economic activity pursued on a permanent for-profit basis) for multilateral trading of DLT securities^{lvii} whose purpose is the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules and which meets at least one of the following criteria: a) It admits participants in accordance with Article 73c paragraph 2 letter e FMIA; b) It holds DLT securities in central custody based on uniform rules and procedures; c) it clears and settles transactions in DLT securities based on uniform rules and procedures (Art. 73a FMIA).^{lviii}

DLT Exchange are subject to part of the duties of an Exchange, i.e. DLT trading facilities are subject to: a) self-regulation (Art. 27 FMIA); b) organisation of trading (Art. 28 FMIA); c) pre- and post-trade transparency (Art. 29 FMIA); d) guarantee of orderly trading (Art. 30 FMIA); e) supervision of trading (Art. 31 FMIA); f) collaboration between trading supervisory bodies (Art. 32 FMIA); g) suspension of trading (Art. 33 para. 2 FMIA); h) appeal body (Art. 37 FMIA) (73b FMIA).

DLT trading facility can admit the following as participants: a) securities firms as defined in Article 41 of the FinIA; b) other parties supervised by FINMA in accordance with Article 3 of the FINSA as well as parties supervised by a foreign authority, provided that the DLT trading facility ensures that they fulfil equivalent technical and operational conditions to securities firms; c) the SNB; d) the Bank for International Settlements (BIS); e) other natural persons and legal entities, provided that they declare that they are participating in their own name and for their own account (Art. 73c FMIA).

Participants domiciled in Switzerland must provide FINMA with all information and documents that it requires to carry out its tasks, while for foreign-domiciled participants the DLT trading facility must ensure that FINMA obtains the relevant information and documents if FINMA so requires (art. 73c para 2 FMIA).

DLT trading facility need to apply the provisions on the record-keeping duty (Art. 38 FMIA) and the reporting duty (Art. 39 FMIA) of participants, if no exception by the Federal Council apply for natural persons and legal entities, provided that they declare that they are participating in their own name and for their own account (Art. 73c para 3 and para 1 lit. e FMIA).

The DLT trading facility shall issue regulations on the admission, duties and exclusion of participants, thereby observing in particular the principle of equal treatment and monitor compliance with the regulations and impose the sanctions provided for contractually in the event of violations (Art. 73c para 5 and 6 FMIA)

The DLT trading facility shall issue regulations on the admission of DLT securities to trading and to the other services it provides, particularly, setting out therein the requirements to be met by the DLT securities and the issuers or third parties in connection with the admission (Art 73d para 1 FMIA). A



DLT trading facility admitting, in addition to DLT securities, further assets to trading or to its other services shall issue regulations on the admission of such assets (Art 73d para 2 FMIA). The DLT trading facility shall monitor compliance with the regulations and impose the sanctions provided for contractually in the event of violations (Art 73d para 4 FMIA).

The Federal Council may: a) require that DLT securities be admitted to DLT trading facilities only if they meet certain minimum requirements, in particular as regards their integrity and the availability of public information; b) specify which DLT securities and other assets must not be admitted to DLT trading facilities in order to protect financial market participants or the stability or integrity of the financial system (Art 73d para 3 FMIA).

For DLT trading facilities that are open to other natural persons and legal entities, provided that they declare that they are participating in their own name and for their own account, the Federal Council may set requirements for the protection of these participants in addition to the requirements under Articles 73b–73d FMIA (Art. 73e para 1 FMIA).

For DLT trading facilities that provide central custody, clearing and settlement services, the Federal Council (or FINMA if needed in order to take account of technology-specific risks) shall set requirements in addition to those under Articles 73a–73d FMIA, based on the requirements for central securities depositories (Arts. 61–73 FMIA) in particular with regard to: a) the central custody, clearing and settlement of DLT securities; b) collateral; c) capital adequacy; d) risk diversification; e) ancillary services; f) liquidity; g) procedure in the event of a participant's default; h) segregation (Art. Art. 73e para 2 FMIA).^{lix}

The SNB may specify requirements for systemically important financial market infrastructures (Article 23 and Art. 73e para 5 FMIA).

9.5.2. Small DLT Trading Facility

The Federal Council may ease the requirements for small DLT trading facilities under Articles 6–21, 27–33 and 37 FMIA for reasons of proportionality and while taking into account the protective purpose of the FMIA, in particular the requirements on: a) separation of the bodies responsible for business management from those responsible for overall management, supervision and control (Art. 8 FMIA); b) the provision of ancillary services not subject to authorisation or approval by virtue of the financial market legislation (Art. 10 FMIA); c) the independence of the self-regulatory organisation (Art. 27 para. 2 FMIA) and of the appeal body (Art. 37 para. 1 FMIA).

DLT trading facilities are deemed to be small if they pose a low risk in terms of the protection of financial market participants and the proper functioning and stability of the financial system, in particular because the number of participants, the trading volume, the volume of custody assets or the clearing and settlement volume is limited according to thresholds set by the Federal Council (Art. 37 para. 2 FMIA).

Small DLT trading facilities are required to disclose the facilitation guaranteed in comparison to the regular DLT facility to their customers according to the rules defined by the Federal Council (Art. 73f para 3 FMIA).

9.6. Conclusion

The paper aimed at introducing general concepts of DLT / Blockchain and comparing existing solutions for the tokenization of real world assets. It has been outlined how several options are possible and the requirements for facilitating the trade of token under the Swiss regulatory framework.

The main difficulties encountered during the writing of this paper were in the lack of time.



It was a great pleasure to work with the supportive teaching individuals at the University of Zurich contributing with their great knowledge in this area of expertise.

10. References

- M. Sutter-Rüdissler, C. Germann, M. Letsch, "David" in der Corporate Governance, EF 4/21 S. 165-170
- S. D. Meyer, B. Schuppli, "Smart contracts" und deren Einordnung in das schweizerische Vertragsrecht, recht 2017 S. 204-224
- F. Edard (2019), 4ème partie : Droit civil / Blockchain et santé : perspectives juridiques en Suisse, CUSO - Programme doctoral romand de droit, S. 215-234
- L. Bianchi, E. Bollinger (2016, CapLaw-2016-47
- P. Vogel, M. Kurak, J. Huebner (2019), Blockchain and Philanthropy, EF 3/19 S, 133-136
- C. Zellwegger-Gutknecht, Einleitung vor Art. 1 ff., BSK OR I-Zellwegger-Gutknecht, Einl. Vor Art. 1ff
- O. Guillor, G. Steffen, Art. 19/20, CR CO I-Guillod/Steffen, Art. 19/20
- C. Müller (2019), Die smart contracts aus Sicht des Schweizerischen Obligationenrechts, ZBJV 155/2019, S. 330-352
- H. Heiss, O. William (2018), ERSTER TEIL Jahrestagung vom 7. September 2018 Schwerpunkt: Privatversicherungsrecht / A. Versicherungsrecht 4.0 / Rechtsfragen der Online-Versicherung / IV. Smart Insurance Contracts, Jahrbuch SGHVR 2018, S. 42-86
- G. Dobrauz, M. A. Schrackmann (2020), Blockchain – innovation et réglementation, EF 12/20 S. 897
- J. Seffinga, M. Grossi, A. Bachmann, T. Hediger (2017), Blockchain in der Praxis, EF 11/17 S. 811-820
- A. Abegg, G. Carle, G. Seferovic (2020), Peer-to-Peer-Systeme bei Zusammenschlüssen zum Eigenverbrauch, JusLetter 14. September 2020
- C. Stengel, R. Aus der Au (2018), Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018 S. 439-452
- M. Plattner (2021), Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Technologie, IMPULSE – Impulse zur praxisorientierten Rechtswissenschaft Band/Nr. 60, S. 17-33
- Lua, E. K., Crowcroft, J., Pias, M., Sharma, R., & Lim, S. (2005). A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys & Tutorials*, 7(2), 72-93
- A. Oram: Peer-to-Peer : Harnessing the Power of Disruptive Technologies
- Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., & Rosenschein, J. S. (2015, May). Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems* (pp. 919-927).
- M. Hess, P. Spielmann (2017), Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht / I.- II., S. 145-173
- Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7, 22328-22370.



M. Simmler, S. Selman, D. Bugermeister (2018), Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 2018 S. 963-978

BGer 4A_581/2020

S. Ahammer (2018), LegalTech 2018: Wo geht es hin?, JusLetter 4. Juni 2018, Rz. 13

L. Müller (2018), Der Bitcoin- und Blockchain-Goldrausch, AJP 2018 S. 680-681

Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1), 1-32.

FINMA Guidance 04/2017, Regulatory Treatment of initial coin offerings, 29. September 2017

S. Oesterhelt, M. Dubach (2019), Besteuerung von ICOs und Kryptowährungen, StR 74/2019, S. 772-784

D. Oesch, H. Petry (2019), Bilanzierung von Kryptowährungen nach Bankenrechnungslegungsvorschriften, EF 1-2/2019 S. 20-23

I. Schwander, Art. 713, BSK ZGB II-Schwander, Art. 713, Rz 6.

L. Meisser, G. Hauser-Spühler (2016), Innovation vs. Regulation, Compliance im Digital-Finance-Bereich, Law & Management Praxis Band/Nr. 6, S. 81-86

T. Linder, M. Molnar (2018), Blockchain, Token und Mehrwertsteuer, EF 12/18 S. 1022-1027

M. F. Huber, S. Guler, J. Dumont (2018), By the same token, StR 73/2018 S. 292-308.

Bullmann, D., Klemm, J., & Pinna, A. (2019). In search for stability in crypto-assets: are stablecoins the solution?. *ECB Occasional Paper*, (230).

C. Jeger, B. Rodrigues, E. Scheid and B. Stiller, "Analysis of Stablecoins during the Global COVID-19 Pandemic," *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 2020, pp. 30-37, doi: 10.1109/BCCA50787.2020.9274450.

P. de Preux, D. Trajilovic (2018), Blockchain et lutte contre le blanchiment d'argent, EF 1-2/18 S. 64-71

Fabian Vogelsteller, Vitalik Buterin, "EIP-20: Token Standard," *Ethereum Improvement Proposals*, no. 20, November 2015. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-20>.

Witek Radomski, Andrew Cooke, Philippe Castonguay, James Therien, Eric Binet, Ronan Sandford, "EIP-1155: Multi Token Standard," *Ethereum Improvement Proposals*, no. 1155, June 2018. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-1155>

R. Kogens, C. Luchsinger Gähwiler (2018), Ein 360-Grad-Blick auf Token, EF 8/18 S. 589-596

M. Aref, L. Fabian, S. Weber (2021), Digitale Originale dank NFTs?, GesKR 2021 S. 385-399

G. Abegg, F. Engelhardt (2019), China takes online dispute resolution to the next level, JusLetter 4. März 2019

A. Sesing, J. S. Baumann (2020), Automatisierung von Vertragsbeziehungen in der Industrie 4.0, InTeR 2020 S. 134-141

T. R. Rohner, C. Jaag (2017), Bitcoin – Steuerlicher Umgang mit Kryptowährungen, NZZ Nr. 2 04.01.2017



- A. Keller, R. Hofstetter, C. Hösli, N. Memmishofer (2021), Crypto Custody, EF 8/21 S. 374-378
- L. Müller, M. Ong (2020), Aktuelles zum Recht der Kryptowährungen, AJP 2020 S. 198-212
- C. Stengel, R. Aus der Au (2018), Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018 S. 439-452
- S. Wolf, W. Wiegand, Vorbemerkungen zu Art. 641 ff, BSK ZGB II-Wolf/Wiegand, Vor Art. 641, Rz 19c
- A.-N. Bandi-Lang, Y. Mauchle, P. Spoerle (2021), Bucheffekten auf der Blockchain, GesKR 2021, S. 238-248
- P. Maume, M. Fromberger (2021), ZHR 185 (2021) S. 507-526
- M. Sutter-Rüdisser, C. Germann, M. Letsch, "David" in der Corporate Governance, EF 4/21 S. 165-170
- B. Hürlimann-Kaup, Aussonderung von Bitcoins im Konkurs des Verwahrers?, AJP 2018 S. 1447-1449
- M. Meuldijk, T. Wattenhofer, Auswirkungen der Digitalisierung auf den Beruf des Wirtschaftsprüfers, EF 11/17 S. 766-772
- S. Zogg (2019), Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, recht 2019 S. 95-120
- M. Eggen (2017), Chain of contracts, AJP 2017 S. 3-15, 4; A. F. Wagner, R. H. Weber (2017), Corporate Governance auf der Blockchain, SZW 2017 S. 59-70
- N. Jacquemart, S. D. Meyer (2017), Der Bitcoin-/Bitcoin-Cash-Hardfork, GesKR 2017 S. 469-485
- S. D. Meyer, B. Schuppli, "Smart contracts" und deren Einordnung in das schweizerische Vertragsrecht, recht 2017 S. 204-224
- A. Lombard (2019), Allgemeines Zivil- und Zivilprozessrecht / Smart Property and the Blockchain, Digitalisierung – Gesellschaft – Recht, S. 243-260
- S. Louven (2018), Antitrust by Desing – Kartellrechtliche Technik-Compliance für Algorithmen, Blockchain und Plattformen?, InTeR 2018 S. 176-178
- J. Oertle (2020), Auswirkungen digitaler Technologien auf Immobilientransaktionen von institutioneller Anlegern, SREJ 20/2020 S. 25-33
- N. Mosimann (2019), Blockchain Technologie als Heilsbringerin für Authentizität und Provenienz? Eine nüchterne Betrachtung, SKR – Schriftenreihe Kultur & Recht Band/Nr 11, S. 139-154
- M. P. A. Müller (2019), Blockchain und Gesellschaftsrecht: Ein Streifzug durch Möglichkeiten und Hürden, EF 6-7/19 S. 485-489
- M. Molnar, T. Linder (2019), Blockchain und Mehrwertsteuer: Verstehen Sie "Kybernetisch"?, EF 1-2/19, S. 84-87
- O. Peltzer, B. Weber-Steinhaus, A. L. Wülbern-Ahmad (2018), Blockchain, Zoll Revue 2/2018 S. 3-10
- A. Kerkemeyer (2020), Blockchain-Transaktionen im internationalen Recht, ZHR 184 (2020) S. 793-829
- T. Koller, Anhang zu Art. 466-471: Das Dokumentenakkreditiv, BSK OR I-Koller, Anh. Art. 466-471
- T. Buff, M. Eggen (2018), Tagungsbericht zur Veranstaltung "Notariat und digitale Welt" am Notariatstag 2018 des Verbandes bernischer Notare, JusLetter 2. Juli 2018



- F. Contratto (2016), "Reg Tech": Digitale Wende für Aufsicht und Compliance, JusLetter 15. August 2016
- L. Forrer, F. Zuur, M. P. A. Müller (2020), Das Aktienrecht im Wandel der Digitalisierung – Entstehung der Gesellschaft, Willensbildung der Organe und Blockchain Technologie, S. 1-27
- O. D. William (2019), Digitalisierung im Versicherungsvertragsrecht, HAVE 2019 S. 83-89
- D. Hillemann, G. Wiebe (2020), Einsatzmöglichkeiten der Blockchain Technologie im Produktsicherheitsrecht, CB 2020 S. 455-460
- J. Essebier, D. A. Wyss (2017), Von der Blockchain zu Smart Contracts, Jusletter 24. April 2017
- P. Favrod-Coune, V. Pignon (2021), La Fintech en Suisse Aspects réglementaires et économiques, LaPD – La pratique du Droit, S. 93-106
- T. Müller (2018), Die ICO-Community muss erwachsen werden, NZZ Nr. 82 10.04.2018 S. 12
- J. Essebier, J. Bourgeois (2018), Die Regulierung von ICOs, AJP 2018 S. 568-579
- J. Iffland, A. Läser (2018), Die Tokenisierung von Effekten, GesKR 2018 S. 415-423
- F. Schurr (2019), Anbahnung, Abschluss und Durchführung von Smart Contracts im Rechtsvergleich, ZGglRWiss 2019, S. 257-284
- Y. Mauchle (2017), Die regulatorische Antwort auf FinTech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen, SZW 2017 S. 810-830
- A. Abegglen, F. Andreotti (2020), Best Execution gemäss FIDLEG, GesKR 2020 S. 36-59
- FINMA circular 2018/01 Organised Trading Facility, Rz 31-35
- H. C. von der Crone, M. Derungs (2019), Aktien als digitalisierte Werte, SZW 2019 S. 481-497
- H. C. von der Crone, M. Monsch, L. Meisser (2019), Aktien-Token, GesKR 2019 S. 1-17
- P. Märkl, A. von Rosenstiel (2021), Blockchain arbitration und dezentralisierte Streibeilegung, ZVglRWiss 2021 S. 257-269
- U. Bertschinger (2019) Das Finanzmarktaufsichtsrecht vom vierten Quartal 2018 bis ins vierte Quartal 2019, SZW 2019 S. 676-696
- L. Bianchi, F. Andreotti (2019), Digital Assets – proposed amendments to the legal and regulatory framework of distributed ledger technology in Switzerland, CapLaw-2019-15
- S. Kramer, U. Meier (2020), DLT Draft Law – civil law aspects, CapLaw-2020-2
- M. Eggen, C. Sillaber (2020), DLT-Handelssysteme, Jusletter 11. Mai 2020, Rz. 4ff
- S. Sulzer (2019), Banken- und Kapitalmarktrecht / II. Bedeutung für die Schweiz, Wirtschaftsrecht Schweiz-EU Überblick und Kommentar 2018/19 S. 22-44
- N. B. Binder, T. Burri, M. F. Lohmann, M. Simmler, F. Thouvenin, K. N. Vokinger (2021), Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht, JusLetter 28. Juni 2021
- R. Sethe, D. Lütolf (2020), Entwicklungen im Gesellschaftsrecht und im Wertpapierrecht, SJZ 116/2020 S. 709-715
- Cfr. J. Iffland, A. B. Hattar (2020) Central securities depositories in the age of tokenized securities, CapLaw-2020-5



11. Webreferences

<https://bitcoin.org/bitcoin.pdf>

<https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/>

<https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/finanztechnologie-und-digitalisierung-2016/>

<https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>

<https://vittominacori.github.io/erc20-generator/>

<https://docs.openzeppelin.com/contracts/3.x/tokens#ERC20>

<https://eips.ethereum.org/EIPS/eip-721>

<https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>

<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/ERC721.sol>

<https://docs.openzeppelin.com/contracts/3.x/erc721>

<https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/>

<https://docs.openzeppelin.com/contracts/3.x/erc1155>

<https://eips.ethereum.org/EIPS/eip-1155>

<https://enjin.io/erc-1155>; <https://github.com/enjin/erc-1155>

<https://coinspot.zendesk.com/hc/en-us/articles/360001006696-What-are-different-token-standards->

ⁱ <https://bitcoin.org/bitcoin.pdf>; cfr. M. Sutter-Rüdissler, C. Germann, M. Letsch, “David” in der Corporate Governance, EF 4/21 S. 165-170, 166; S. D. Meyer, B. Schuppli, “Smart contracts” und deren Einordnung in das schweizerische Vertragsrecht, recht 2017 S. 204-224, 205; F. Edard (2019), 4ème partie : Droit civil / Blockchain et santé : perspectives juridiques en Suisse, CUSO - Programme doctoral romand de droit, S. 215-234, 218; L. Bianchi, E. Bollinger (2016, CapLaw-2016-47.

ⁱⁱ Cfr. P. Vogel, M. Kurak, J. Huebner (2019), Blockchain and Philantropy, EF 3/19 S, 133-136, 133; C. Zellwegger-Gutknecht, Einleitung vor Art. 1 ff., BSK OR I-Zellwegger-Gutknecht, Einl. Vor Art. 1ff, Rz 39; O. Guillor, G. Steffen, Art. 19/20, CR CO I-Guillod/Steffen, Art. 19/20, Rz 112; C. Müller (2019), Die smart contracts aus Sicht des Schweizerischen Obligationenrechts, ZBJV 155/2019, S. 330-352, 333; H. Heiss, O. William (2018), ERSTER TEIL Jahrestagung vom 7. September 2018 Schwerpunkt: Privatversicherungsrecht / A. Versicherungsrecht 4.0 / Rechtsfragen der Online-Versicherung / IV. Smart Insurance Contracts, Jahrbuch SGHVR 2018, S. 42-86, 43

ⁱⁱⁱ Cfr. G. Dobrauz, M. A. Schrackmann (2020), Blockchain – innovation et réglementation, EF 12/20 S. 897 ; J. Seffinga, M. Grossi, A. Bachmann, T. Hediger (2017), Blockchain in der Praxis, EF 11/17 S. 811-820, 812.

^{iv} Cfr. for the example of P2P for electricity, A. Abegg, G. Carle, G. Seferovic (2020), Peer-to-Peer-Systeme bei Zusammenschlüssen zum Eigenverbrauch, JusLetter 14. September 2020.



-
- ^v Cfr. C. Stengel, R. Aus der Au (2018), Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018 S. 439-452; M. Plattner (2021), Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Technologie, IMPULSE – Impulse zur praxisorientierten Rechtswissenschaft Band/Nr. 60, S. 17-33, 21
- ^{vi} Lua, E. K., Crowcroft, J., Pias, M., Sharma, R., & Lim, S. (2005). A survey and comparison of peer-to-peer overlay network schemes. *IEEE Communications Surveys & Tutorials*, 7(2), 72-93.
- ^{vii} A. Oram: Peer-to-Peer : Harnessing the Power of Disruptive Technologies
- ^{viii} <https://bitcoin.org/bitcoin.pdf>
- ^{ix} <https://bitcoin.org/bitcoin.pdf>
- ^x Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., & Rosenschein, J. S. (2015, May). Bitcoin mining pools: A cooperative game theoretic analysis. In *Proceedings of the 2015 International Conference on Autonomous Agents and Multiagent Systems* (pp. 919-927).
- ^{xi} Cfr. M. Hess, P. Spielmann (2017), Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht / I.- II., S. 145-173, 158
- ^{xii} Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access*, 7, 22328-22370.
- ^{xiii} Cfr. M. Simmler, S. Selman, D. Bugermeister (2018), Beschlagnahme von Kryptowährungen im Strafverfahren, AJP 2018 S. 963-978, 964; cfr. for smart contract in Swiss Jurisprudence, BGer 4A_581/2020; S. Ahammer (2018), LegalTech 2018: Wo geht es hin?, JusLetter 4. Juni 2018, Rz. 13; L. Müller (2018), Der Bitcoin- und Blockchain-Goldrausch, AJP 2018 S- 680-681, 680
- ^{xiv} Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, 7(1), 1-32.
- ^{xv} FINMA Guidance 04/2017, Regulatory Treatment of initial coin offerings, 29. September 2017, 1; cfr. S. Oesterhelt, M. Dubach (2019), Besteuerung von ICOs und Kryptowährungen, StR 74/2019, S. 772-784, 772; D. Oesch, H. Petry (2019), Bilanzierung von Kryptowährungen nach Bankenrechnungslegungsvorschriften, EF 1-2/2019 S. 20-23, 21; I. Schwander, Art. 713, BSK ZGB II-Schwander, Art. 713, Rz 6.
- ^{xvi} FINMA Guidance 04/2017, Regulatory Treatment of initial coin offerings, 29. September 2017, 1; different opinion L. Meisser, G. Hauser-Spühler (2016), Innovation vs. Regulation, Compliance im Digital-Finance-Bereich, Law & Management Praxis Band/Nr. 6, S. 81-86, 82
- ^{xvii} <https://www.finma.ch/en/news/2017/09/20170919-mm-coin-anbieter/>
- ^{xviii} <https://www.finma.ch/de/dokumentation/dossier/dossier-fintech/finanztechnologie-und-digitalisierung-2016/>
- ^{xix} FINMA ICO guidelines; alternative token classification, T. Linder, M. Molnar (2018), Blockchain, Token und Mehrwertsteuer, EF 12/18 S. 1022-1027, 1024; M. F. Huber, S. Guler, J. Dumont (2018), By the same token, StR 73/2018 S. 292-308, 294.
- ^{xx} FINMA ICO guidelines, Appendix
- ^{xxi} Bullmann, D., Klemm, J., & Pinna, A. (2019). In search for stability in crypto-assets: are stablecoins the solution?. *ECB Occasional Paper*, (230).
- ^{xxii} C. Jeger, B. Rodrigues, E. Scheid and B. Stiller, "Analysis of Stablecoins during the Global COVID-19 Pandemic," *2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, 2020, pp. 30-37, doi: 10.1109/BCCA50787.2020.9274450.
- ^{xxiii} SR 952.0
- ^{xxiv} SR 951.31
- ^{xxv} SR 958.1
- ^{xxvi} SR 955.0; cfr. P. de Preux, D. Trajilovic (2018), Blockchain et lutte contre le blanchiment d'argent, EF 1-2/18 S. 64-71, 64



-
- xxvii [Fabian Vogelsteller](#), [Vitalik Buterin](#), "EIP-20: Token Standard," *Ethereum Improvement Proposals*, no. 20, November 2015. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-20>.
- xxviii <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>
- xxix <https://vittominacori.github.io/erc20-generator/>
- xxx [Fabian Vogelsteller](#), [Vitalik Buterin](#), "EIP-20: Token Standard," *Ethereum Improvement Proposals*, no. 20, November 2015. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-20>.
- xxxi <https://ethereum.org/en/developers/docs/standards/tokens/erc-20/>
- xxxii <https://docs.openzeppelin.com/contracts/3.x/tokens#ERC20>
- xxxiii <https://eips.ethereum.org/EIPS/eip-721>
- xxxiv <https://ethereum.org/en/developers/docs/standards/tokens/erc-721/>;
<https://github.com/OpenZeppelin/openzeppelin-contracts/blob/master/contracts/token/ERC721/ERC721.sol>
- xxxv Cfr. <https://docs.openzeppelin.com/contracts/3.x/erc721>
- xxxvi [Witek Radomski](#), [Andrew Cooke](#), [Philippe Castonguay](#), [James Therien](#), [Eric Binet](#), [Ronan Sandford](#), "EIP-1155: Multi Token Standard," *Ethereum Improvement Proposals*, no. 1155, June 2018. [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-1155>.
- xxxvii <https://ethereum.org/en/developers/docs/standards/tokens/erc-1155/>;
<https://docs.openzeppelin.com/contracts/3.x/erc1155>
- xxxviii <https://eips.ethereum.org/EIPS/eip-1155>
- xxxix <https://enjin.io/erc-1155>; <https://github.com/enjin/erc-1155>
- xl <https://coinspot.zendesk.com/hc/en-us/articles/360001006696-What-are-different-token-standards->
- xli <https://coinspot.zendesk.com/hc/en-us/articles/360001006696-What-are-different-token-standards->
- xlii Cfr. R. Kogens, C. Luchsinger Gähwiler (2018), Ein 360-Grad-Blick auf Token, EF 8/18 S. 589-596, 589
- xliii In principle, exception is made for a five euro bill that was physically amended (e.g. cut), is part of a dedicated series (e.g. printed with a specific design, that has been later updated).
- xliv M. Aref, L. Fabian, S. Weber (2021), Digitale Originale dank NFTs?, GesKR 2021 S. 385-399, 387
- xliv Cfr. G. Abegg, F. Engelhardt (2019), China takes online dispute resolution to the next level, JusLetter 4. März 2019, S. 6; A. Sesing, J. S. Baumann (2020), Automatisierung von Vertragsbeziehungen in der Industrie 4.0, InTeR 2020 S. 134-141, 137; T. R. Rohner, C. Jaag (2017), Bitcoin – Steuerlicher Umgang mit Kryptowährungen, NZZ Nr. 2 04.01.2017, S. 10; re. the risks, A. Keller, R. Hofstetter, C. Hösli, N. Memmishofer (2021), Crypto Custody, EF 8/21 S. 374-378, 375.
- xlvi L. Müller, M. Ong (2020), Aktuelles zum Recht der Kryptowährungen, AJP 2020 S. 198-212, 199; C. Stengel, R. Aus der Au (2018), Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018 S. 439-452, 441; S. Wolf, W. Wiegand, Vorbemerkungen zu Art. 641 ff, BSK ZGB II-Wolf/Wiegand, Vor Art. 641, Rz 19c; A.-N. Bandi-Lang, Y. Mauchle, P. Spoerle (2021), Bucheffekten auf der Blockchain, GesKR 2021, S. 238-248, 239; P. Maume, M. Fromberger (2021), ZHR 185 (2021) S. 507-526, 511
- xlvii cfr. M. Sutter-Rüdisser, C. Germann, M. Letsch, "David" in der Corporate Governance, EF 4/21 S. 165-170, 167; B. Hürlimann-Kaup, Aussonderung von Bitcoins im Konkurs des Verwahrers?, AJP 2018 S. 1447-1449, 1448; M. Meuldijk, T. Wattenhofer, Auswirkungen der Digitalisierung auf den Beruf des Wirtschaftsprüfers, EF 11/17 S. 766-772, 769; S. Zogg (2019), Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, recht 2019 S. 95-120, 96; M. Eggen (2017), Chain of contracts, AJP 2017 S. 3-15, 4; A. F. Wagner, R. H. Weber (2017), Corporate Governance auf der Blockchain, SZW 2017 S. 59-70, 61; N. Jacquemart, S. D. Meyer (2017), Der Bitcoin-/Bitcoin-Cash-Hardfork, GesKR 2017 S. 469-485, 470



^{xlvi} S. D. Meyer, B. Schuppli, “Smart contracts” und deren Einordnung in das schweizerische Vertragsrecht, *recht* 2017 S. 204-224, 209; cfr. A. Lombard (2019), *Allgemeines Zivil- und Zivilprozessrecht / Smart Property and the Blockchain, Digitalisierung – Gesellschaft – Recht*, S. 243-260, 256; S. Louven (2018), *Antitrust by Desing – Kartellrechtliche Technik-Compliance für Algorithmen, Blockchain und Plattformen?*, *InTeR* 2018 S. 176-178, 177; J. Oertle (2020), *Auswirkungen digitaler Technologien auf Immobilientransaktionen von institutioneller Anlegern*, *SREJ* 20/2020 S. 25-33, 30; N. Mosimann (2019), *Blockchain Technologie als Heilsbringerin für Authentizität und Provenienz? Eine nüchterne Betrachtung*, *SKR – Schriftenreihe Kultur & Recht* Band/Nr 11, S. 139-154, 140; M. P. A. Müller (2019), *Blockchain und Gesellschaftsrecht: Ein Streifzug durch Möglichkeiten und Hürden*, *EF* 6-7/19 S. 485-489, 486; M. Molnar, T. Linder (2019), *Blockchain und Mehrwertsteuer: Verstehen Sie “Kybernetisch”?*, *EF* 1-2/19, S. 84-87, 84; O. Peltzer, B. Weber-Steinhaus, A. L. Wülbern-Ahmad (2018), *Blockchain*, *Zoll Revue* 2/2018 S. 3-10, 4; A. Kerkemeyer (2020), *Blockchain-Transaktionen im internationalen Recht*, *ZHR* 184 (2020) S. 793-829, 797; T. Koller, Anhang zu Art. 466-471: *Das Dokumentenakkreditiv*, *BSK OR I-Koller, Anh. Art. 466-471, Rz* 2b; T. Buff, M. Eggen (2018), *Tagungsbericht zur Veranstaltung “Notariat und digitale Welt” am Notariatstag 2018 des Verbandes bernischer Notare*, *JusLetter* 2. Juli 2018, *Rz* 2; F. Contratto (2016), *“Reg Tech”: Digitale Wende für Aufsicht und Compliance*, *JusLetter* 15. August 2016, *Rz* 2; L. Forrer, F. Zuur, M. P. A. Müller (2020), *Das Aktienrecht im Wandel der Digitalisierung – Entstehung der Gesellschaft, Willensbildung der organe und Blockchain Technologie*, S. 1-27, 7; O. D. William (2019), *Digitalisierung im Versicherungsvertragsrecht*, *HAVE* 2019 S. 83-89, 87; D. Hillemann, G. Wiebe (2020), *Einsatzmöglichkeiten der Blockchain Technologie im Produktsicherheitsrecht*, *CB* 2020 S. 455-460, 455; J. Essebier, D. A. Wyss (2017), *Von der Blockchain zu Smart Contracts*, *Jusletter* 24. April 2017, *Rz* 19.

^{xliv} Cfr. P. Favrod-Coune, V. Pignon (2021), *La Fintech en Suisse Aspects réglementaires et économiques*, *LaPD – La pratique du Droit*, S. 93-106, 94; T. Müller (2018), *Die ICO-Community muss erwachsen werden*, *NZZ* Nr. 82 10.04.2018 S. 12 ; J. Essebier, J. Bourgeois (2018), *Die Regulierung von ICOs*, *AJP* 2018 S. 568-579, S. 568; J. Iffland, A. Läser (2018), *Die Tokenisierung von Effekten*, *GesKR* 2018 S. 415-423, 415.

^l F. Schurr (2019), *Anbahnung, Abschluss und Durchführung von Smart Contracts im Rechtsvergleich*, *ZGglRWiss* 2019, S. 257-284, 262

^{li} Art. 65 para 1 FinIO.

^{lii} Art. 65 para 4 FinIO.

^{liii} Cfr. Y. Mauchle (2017), *Die regulatorische Antwort auf FinTech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen*, *SZW* 2017 S. 810-830, S. 818.

^{liiv} Cfr. A. Abegglen, F. Andreotti (2020), *Best Execution gemäss FIDLEG*, *GesKR* 2020 S. 36-59, 52

^{lv} FINMA circular 2018/01 *Organised Trading Facility*, *Rz* 31-35

^{lvi} FINMA circular 2018/01, *Rz*. 36ff.

^{lvii} Cfr. H. C. von der Crone, M. Derungs (2019), *Aktien als digitalisierte Werte*, *SZW* 2019 S. 481-497, 487; H. C. von der Crone, M. Monsch, L- Meisser (2019), *Aktien-Token*, *GesKR* 2019 S. 1-17, 14; P. Märkl, A. von Rosenstiel (2021), *Blockchain arbitration und dezentralisierte Streibeilegung*, *ZVglRWiss* 2021 S. 257-269, 262; U. Bertschinger (2019) *Das Finanzmarktaufsichtsrecht vom vierten Quartal 2018 bis ins vierte Quartal 2019*, *SZW* 2019 S. 676-696, 684; L. Bianchi, F. Andreotti (2019), *Digital Assets – proposed amendments to the legal and regulatory framework of distributed ledger technology in Switzerland*, *CapLaw-2019-15*; S. Kramer, U. Meier (2020), *DLT Draft Law – civil law aspects*, *CapLaw-2020-2*

^{lviii} Cfr. M. Eggen, C. Sillaber (2020), *DLT-Handelssysteme*, *Jusletter* 11. Mai 2020, *Rz*. 4ff; S. Sulzer (2019), *Banken- und Kapitalmarktrecht / II. Bedeutung für die Schweiz*, *Wirtschaftsrecht Schweiz-EU Überblick und Kommentar* 2018/19 S. 22-44, 29; N. B. Binder, T. Burri, M. F. Lohmann, M. Simmler, F. Thouvenin, K. N. Vokinger (2021), *Künstliche Intelligenz: Handlungsbedarf im Schweizer Recht*, *JusLetter* 28. Juni 2021; R. Sethe, D. Lütolf (2020), *Entwicklungen im Gesellschaftsrecht und im Wertpapierrecht*, *SJZ* 116/2020 S. 709-715, *Rz*. G.



**Universität
Zürich**^{UZH}

CAS Blockchain

^{lix} Cfr. J. Iffland, A. B. Hattar (2020) Central securities depositories in the age of tokenized securities, CapLaw-2020-5