Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Council

Bern, 14 December 2018

Legal framework for distributed ledger technology and blockchain in Switzerland

An overview with a focus on the financial sector

Federal Council report

Table of contents

1 Introduction 11

1.1 Background and objective of the report 11
1.2 General comments on the report 12
1.3 Principles of the Swiss regulatory approach to blockchain and DLT 12
1.4 Development and structure of the report 14
1.5 Other relevant framework conditions 14

2 Fundamentals of DLT/blockchain 17

2.1 Introduction 17
2.2 Fundamentals of DLT using the example of Bitcoin 17
2.3 Design of a DLT systems 21
2.3.1 Application and flexibility 21
2.3.2 Access 22
2.3.3 Consensus mechanism 23
2.3.4 Log structure 24
2.3.5 Anonymity and privacy 24
2.3.6 Scaling 25
2.4 Stakeholders in the DLT world 25
2.5 Technological obstacles 27
2.5.1 Possible design trade-offs 27
2.5.2 Operational risks 28

3 Applications of DLT in the financial sector 31

3.1 Introduction 31
3.2 Corporate and project financing through initial coin offerings (ICOs) 31
3.2.1 Preliminary remarks 31
3.2.2 Market size worldwide and in Switzerland 31
3.2.3 How ICOs work 32
3.2.4 Characteristics of tokens 34
3.2.5 Potential of ICOs 34
3.3 Payment transactions 34
3.3.1 Preliminary remarks 34
3.3.2 DLT in payment transactions 35
3.3.3 Potential of DLT 35
3.3.3.1 Domestic payment transactions 35
3.3.3.2 Cross-border payment transactions 36
3.4 Securities trading, clearing, and settlement 36
3.4.1 DLT in securities trading, clearing, and settlement 36
3.4.2 Potential of DLT 36
3.4.3 Payment tokens for settling securities transactions 37
3.4.3.1 Instability of value and credit risk of payment tokens 37
3.4.3.2 Possible design of a payment token for settling securities transactions 38
3.5 Asset management 38
3.6 Trade finance 38
3.7 Insurers 40
3.8 Regulatory disclosure and reporting 40

4 International environment 41

4.1 Developments at the international level 41
4.2 Multilateral developments 41
4.3 Switzerland's positioning in multilateral bodies in the financial area 42

5 Legal basis under civil law 44

5.1 Legal classification and transfer of tokens 44
5.1.1 Data ownership rights 44
5.1.1.1 The situation under current law 44
5.1.1.2 The question of introducing the concept of data ownership 44
5.1.1.3 Ownership rights to tokens? 45
5.1.2 Legal classification of tokens by content 46
5.1.2.1 General principles 46
5.1.2.2 Claims 46
5.1.2.3 Membership in a company 47
a) Limits on company structure 47
b) Possibility of linking tokens to membership of a company 48
5.1.2.4 Rights in rem 49
a) Principle: Embodiment of rights in rem through ownership 49
b) Separation of ownership and direct possession 49
c) Conclusion 50
5.1.2.5 Cryptocurrencies 50
a) Intangible assets 50
b) Money? 51
5.1.3 Classification by wrapper: Negotiable securities, uncertificated securities, and intermediated securities 52
5.1.3.1 Background 52
5.1.3.2 Certificated securities 53
a) Definition and creation of certificated securities 53
b) Securitised rights 54
c) Effects of securitisation 55
d) Tokens as certificated securities *de lege lata*? 56
5.1.3.3 Uncertificated securities 57
a) Definition and creation of uncertificated securities 57
b) Effects of design as an uncertificated security 57
c) Tokens as uncertificated securities *de lege lata* 58
5.1.3.4 Intermediated securities 58
5.1.4 Transfer of tokens 59
5.1.4.1 General principles 59
5.1.4.2 Simple claims and uncertificated securities 59
a) Assignment 59
b) Assumption of contract 60
c) Conclusion 61
5.1.4.3 Property (including certificated securities) 61
a) Principle: Physical delivery (*traditio*) 61
b) Providing the means to gain effective control of an object 62
c) Transfer of possession by means of a legal transaction (surrogates for physical delivery) 62
d) Conclusion 63
5.1.4.4 Intermediated securities 63
5.1.4.5 Cryptocurrencies 63
5.1.5 Conclusion 63
5.2 Treatment of crypto assets and data in insolvency proceedings 65
5.2.1 Statement of the problem 65
5.2.2 Segregation of crypto assets in bankruptcy – current law 65
5.2.2.1 General principles 65
5.2.2.2 Inclusion in the bankruptcy estate 66
5.2.2.3 Segregation under Article 242 DEBA 67
5.2.2.4 Conclusion 68
5.2.3 Extension to all data 69

5.2.4 Conclusion....70
5.3 Private International Law....70
5.3.1 Preliminary remarks....70
5.3.2 Jurisdiction of the Swiss courts....71
5.3.2.1 Contractual designation of the place of jurisdiction....71
5.3.2.2 Tokens linked to a claim....71
5.3.2.3 Tokens linked to membership....72
5.3.2.4 Tokens linked to a right in rem....72
5.3.2.5 Prospectus liability actions....73
5.3.2.6 Reselling of a token....73
5.3.2.7 Tokens as cryptocurrencies....74
5.3.3 Applicable law....74
5.3.3.1 Extensive choice of law....74
5.3.3.2 Tokens linked to a claim....74
5.3.3.3 Tokens linked to membership....75
5.3.3.4 Tokens linked to a right in rem....75
5.3.3.5 Prospectus liability actions....76
5.3.3.6 Reselling or pledging of a token....76
5.3.3.7 Tokens as cryptocurrencies....77
5.3.4 Recognition of foreign judgments....77
5.3.5 Conclusion....78
5.4 Other legal questions....78
5.4.1 Data protection aspects of the blockchain....78
5.4.2 Registers on the blockchain....80
5.4.3 Smart Contracts....80
6 Financial market law....82
6.1 Introduction....82
6.1.1 Overview....82
6.1.2 The role of FINMA's fintech desk....82
6.2 Classification of tokens pursuant to financial market law....83
6.2.1 Introduction....83
6.2.2 Asset tokens....83
6.2.3 Utility tokens....83
6.2.4 Payment tokens....84
6.2.5 Conclusion....84
6.3 Banking Act (BankA)....84
6.3.1 Introduction....84
6.3.2 Bank authorisation requirement and exemptions relevant for blockchain business models....85
6.3.2.1 Bank authorisation requirement....85
6.3.2.2 Exceptions (no bank authorisation needed)....86
6.3.2.3 New authorisation category in banking law (fintech authorisation)....89
6.3.3 Treatment of tokens under bank insolvency law....90
6.3.3.1 Preliminary remarks....90
6.3.3.2 Tokens as deposits....90
6.3.3.3 Tokens as custody assets....90
6.3.4 Extension of the term "deposit" specifically with respect to tokens?....91
6.3.5 Point of contact: Capital requirements for tokens....92
6.3.6 Conclusion....92
6.4 Financial Market Infrastructure Act (FMIA)....92
6.4.1 Introduction....92
6.4.2 Securities and derivatives terms in financial market infrastructure law....93

6.4.2.1 Background ... 93
6.4.2.2 The term "securities" in the case of tokens ... 94
6.4.2.3 The term "derivatives" for tokens ... 95
6.4.2.4 Interim conclusion: no amendment of the definitions of securities and derivatives ... 96
6.4.3 Financial market infrastructures in the age of blockchain and DLT ... 96
6.4.4 Trading institutions ... 98
6.4.4.1 Overview ... 98
6.4.4.2 Licensing requirement for crypto-trading platforms ... 99
6.4.4.3 Assets traded in trading facilities ... 101
6.4.4.4 Duties of trading institutions ... 102
6.4.4.5 Market players participating in trading institutions (participants) ... 103
6.4.4.6 Duties of the participants in trading facilities ... 104
6.4.5 Payment systems ... 104
6.4.6 Clearing and settlement systems ... 105
6.4.7 Innovation areas in financial market infrastructure law and the creation of a new authorisation category ... 107
6.4.7.1 Innovation areas (sandboxes) in financial market infrastructure law 107
6.4.7.2 Creation of a new authorisation category for financial market infrastructures in the blockchain/DLT area ... 108
6.4.7.3 Outlook: regulation of decentralised financial market "infrastructures" ... 109
6.4.8 Market conduct rules in securities and derivatives trading ... 109
6.4.8.1 General ... 109
6.4.8.2 Trade with derivatives ... 110
6.4.8.3 Disclosure of shareholdings ... 110
6.4.8.4 Public takeover offers ... 110
6.4.8.5 Insider trading and market manipulation ... 111
6.4.9 Conclusion ... 111
6.5 Financial Institutions Act (FinIA) ... 112
6.5.1 Introduction ... 112
6.5.2 Legal situation in accordance with FinIA ... 112
6.5.2.1 Legal basis ... 112
6.5.2.2 Management of tokens ... 114
6.5.2.3 Issue of tokens ... 114
6.5.2.4 Professional trading with tokens ... 114
6.5.3 Conclusion ... 114
6.6 Federal Financial Services Act (FinSA) ... 115
6.6.1 Introduction ... 115
6.6.2 Legal bases ... 115
6.6.2.1 Purpose and scope of FinSA ... 115
6.6.2.2 Financial instruments and securities in accordance with FinSA ... 115
6.6.2.3 Financial services and financial service providers in accordance with FinSA ... 116
6.6.3 Players in the crypto area and FinSA ... 117
6.6.4 ICOs from the FinSA perspective ... 120
6.6.4.1 Initial issue of tokens as a financial service? ... 120
6.6.4.2 Issuer and producer in an ICO ... 120
6.6.4.3 Offer or public offer within the meaning of Article 3 letters g and h FinSA ... 121
6.6.5 FinSA duties in case of an ICO ... 121
6.6.5.1 Prospectus requirement in accordance with Article 35 et seq. FinSA ... 121

6.6.5.2 Content of prospectus in accordance with Article 40 et seq. FinSA 121
6.6.5.3 Exemptions from the prospectus requirement in accordance with Article 36 et seq. FinSA ... 122
6.6.5.4 Key information document (KID) for financial instruments in accordance with Article 58 et seq. FinSA ... 123
6.6.5.5 Review of the prospectus and publication in accordance with Article 51 et seq. and Article 64 et seq. FinSA ... 123
6.6.5.6 Other duties in accordance with FinSA ... 124
6.6.6 Conclusion ... 124
6.7 Collective Investment Schemes Act (CISA) ... 125
6.7.1 Introduction ... 125
6.7.2 Current legal situation ... 125
6.7.2.1 Basic regulatory content of CISA ... 125
6.7.2.2 Regulation of Swiss crypto funds ... 126
6.7.2.3 Distribution of foreign crypto funds in Switzerland ... 127
6.7.2.4 Recording of fund units on a blockchain ... 128
6.7.2.5 Recording of the fund's assets on a blockchain ... 128
6.7.2.6 Decentralised autonomous organisations (DAO) / funds on the blockchain ... 128
6.7.3 Conclusion ... 129
6.8 Insurance and DLT ... 130
7 Combating money laundering and terrorist financing ... 131
7.1 Introduction ... 131
7.2 Terms and legal basis ... 131
7.2.1 Swiss Criminal Code ... 131
7.2.2 Anti-Money Laundering Act and Anti-Money Laundering Ordinance ... 132
7.2.3 FINMA Anti-Money Laundering Ordinance ... 134
7.3 Risks ... 135
7.3.1 Threats in relation to cryptobased assets ... 135
7.3.1.1 Threat inherent in the technology for cryptobased assets ... 135
7.3.1.2 Cryptobased assets and traditional financial crime ... 135
7.3.2 Money laundering and terrorist financing risks in relation to ICOs ... 136
7.3.3 Switzerland's vulnerabilities with regard to money laundering and terrorist financing via cryptobased assets ... 136
7.3.4 Risk analysis conclusion ... 136
7.4 Applicability of the Anti-Money Laundering Act to activities in the crypto area 136
7.4.1 Applicability of the Anti-Money Laundering Act to activities involving cryptocurrencies ... 137
7.4.1.1 Wallet providers ... 137
7.4.1.2 Trading platforms ... 138
7.4.1.3 Currency exchange offices ... 139
7.4.1.4 Crypto funds ... 139
7.4.1.5 Mining ... 139
7.4.2 Applicability of anti-money laundering legislation to activities involving ICOs ... 139
7.4.2.1 Payment tokens ... 139
7.4.2.2 Asset tokens ... 140
7.4.2.3 Utility tokens ... 140
7.5 Conclusion ... 140

8 Summary of the comments received in the informal industry consultation 143

9 Reference lists.....145

9.1 Bibliography 145
9.2 List of materials.....155
9.3 Abbreviations 159

Executive summary

Preface

Distributed ledger technology (DLT) and blockchain technologies are among the remarkable and potentially promising developments in digitalisation. It is predicted that these developments have considerable potential for innovation and enhanced efficiency, both in the financial sector and in other sectors of the economy, although this potential cannot yet be conclusively estimated. Switzerland is currently one of the leading locations in the area of DLT and blockchain. Especially in the financial sector, a growing fintech and blockchain ecosystem has developed in Switzerland in recent years.

The Federal Council intends to further improve the prerequisites so that Switzerland can exploit the opportunities offered by digitalisation. It thus wants to create the best possible framework conditions so that Switzerland can establish itself and evolve as a leading, innovative and sustainable location for fintech and blockchain companies – and innovative companies in general. At the same time, the Federal Council attaches great importance to ensuring the integrity and reputation of Switzerland as a financial centre and business location.

With this report, the Federal Council aims to provide an overview of the relevant legal framework and to clarify the need for action. In addition, the report should send a signal and show (i) that Switzerland is open to technological developments such as DLT and blockchain, (ii) that the Swiss legal framework is already suitable for dealing with business models based on DLT and blockchain, (iii) that Switzerland wants to further improve the innovation-friendly framework conditions and (iv) that the Swiss authorities are determined to rigorously combat abuses.

The Federal Council has based this report on the following principles:

(i) Policymakers should provide an optimal framework conducive to innovation, while market and society preferences should determine which technologies will prevail;

(ii) Switzerland should not fundamentally call into question its proven and balanced legal framework, but should swiftly make targeted adjustments as needed where there are gaps or obstacles with regard to DLT/blockchain applications;

(iii) Switzerland should continue to pursue a principle-based and technology-neutral legislative and regulatory approach, but should also allow exceptions if necessary; the rules should be as competition-neutral as possible;

(iv) Switzerland should position itself as an attractive location vis-à-vis DLT/blockchain companies by means of legal certainty, efficient regulation and a good reputation, whereby the use of innovative technologies for fraudulent or abusive acts or to circumvent the regulatory framework will not be tolerated; and

(v) Swiss authorities should position themselves as open towards new technologies and innovations such as blockchain and DLT and cultivate regular dialogue with the industry.

This report is based on the analyses of the blockchain/ICO working group, appointed by the Federal Department of Finance (FDF) in January 2018. It identifies courses of action and proposes concrete next steps.

Civil law and insolvency law

From a civil law viewpoint, two types of token can be distinguished. First, there are tokens which primarily represent a value within the blockchain context, e.g. cryptocurrencies such as Bitcoins. According to the prevailing view, these tokens are purely factual intangible assets. Civil law imposes no requirements – and accordingly no obstacles – for their transfer. Consequently, there is no need to adapt civil law with regard to the transfer of cryptocurrencies.

The second category of tokens covers those that represent a legal position (claim, membership, right *in rem*). As per the users' intent, these tokens should fulfil a function similar to the function presently and traditionally fulfilled by securities. Since an entry in a decentralised register accessible to interested parties can create publicity similar to the ownership of a security, it seems justified to attach similar legal effects to this entry. The Federal Council is proposing an amendment to securities law to increase legal certainty. The proven principles of securities law should be retained as much as possible. Digital representation and transfer is therefore possible only for those rights which could also be represented by a security and which are freely transferable. The planned legislative amendment should enable the legally secure transfer of uncertificated securities by means of entries in decentralised registers and be designed as technology-neutral as possible.

The Federal Council also recognises the need for legislative action regarding insolvency law. In the course of bankruptcy proceedings, the assets of the bankrupt debtor are collected and realised. In the process, it is regularly necessary to clarify what is to be included in the debtor's assets. This question arises particularly if assets to which the debtor is economically entitled are deposited with third parties and if the debtor has power of disposal over assets to which third parties assert their rights. In the latter case, it has not yet been conclusively clarified whether it is possible to segregate cryptobased assets. The Federal Council thus considers it necessary to provide for unambiguous rules regarding the segregation of crypto-based assets from the bankrupt's estate by analogy to the owner's right to segregation under current law. Such a right would require in any case that these assets could be unambiguously allocated to the third party. Additionally, the Federal Council considers it necessary to examine whether a right to segregation should be created with regard to data without financial value. As part of the planned consultation, the Federal Council will thus propose a legislative amendment that addresses these issues.

Financial market law

Blockchain and DLT-based applications can have numerous points of contact with financial market law, specifically banking law, financial market infrastructure law, collective investment schemes law, insurance law and the future Financial Services Act and Financial Institutions Act. The objectives of financial market law – such as the protection of the functionality of financial markets and customer protection – are as relevant for the activities of DLT/blockchain companies in the financial sector as they are for all other financial players. The Federal Council currently sees no fundamental issues regarding financial market law that specifically concern blockchain/DLT-based applications and would require fundamental adjustments. Swiss financial market law is generally technology-neutral and able to deal with new technologies.

However, targeted adjustments in individual areas appear sensible:

- In *banking law*, the Federal Council – in the light of the aforementioned proposed amendment to the Debt Enforcement and Bankruptcy Act – will examine a corresponding adjustment of bank insolvency law provisions (particularly in the area of the segregation of custody assets) and submit any adjustment proposals in the planned consultation.
- In *financial market infrastructure law*, the Federal Council is proposing the creation of a new authorisation category for infrastructure providers in the blockchain/DLT area. Furthermore, related amendments to the Financial Market Infrastructure Act and the new Financial Institutions Act are to be proposed with the aim of creating more flexibility in order to better meet the requirements of blockchain/DLT applications.

- The Federal Council currently sees no need to amend the *Financial Services Act* (that will enter into force at the start of 2020) due to blockchain/DLT. The designated requirements, for example for informing customers, are particularly relevant for financial instruments based on blockchain/DLT, as such financial instruments are innovative and sometimes difficult to value, and they can experience very sharp fluctuations in value.
- In terms of *collective investment schemes law*, the Federal Council instructed the FDF in September 2018 to prepare a consultation on amending the Collective Investment Schemes Act by mid-2019 in order to allow for a new category of funds (so-called limited qualified investment funds, L-QIFs). As a result, new innovative products could be placed on the market more quickly and cost-effectively in the future. Apart from that, the use of blockchain/DLT in the area of collective investment schemes law is still at an early stage, which is why the need for action cannot yet be conclusively assessed.
- In the *insurance sector*, many blockchain/DLT projects are currently in their infancy. So far, no need for action in terms of financial market law has become evident, but a conclusive assessment is not yet possible. The Federal Council will continue to follow these developments closely.

Combating money laundering and terrorist financing

The risk analysis prepared in 2018 by the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF) shows that, based on the identified threat and vulnerability in Switzerland, there is a risk of cryptobased assets being misused for money laundering and terrorist financing. Nevertheless, the threat and vulnerability identified affect all countries. However, the risk analysis also shows that the actual risk cannot be determined precisely in Switzerland due to the small number of cases.

The Anti-Money Laundering Act is currently sufficiently technology-neutral to also cover activities related to cryptocurrencies and initial coin offerings (ICOs) to a large extent. The general principles of the Anti-Money Laundering Act also apply to cryptobased assets. The activities of most players in the crypto sector already qualify as financial intermediation and are therefore subject to the Anti-Money Laundering Act. The scope of the Anti-Money Laundering Act is thus already relatively comprehensive by international comparison. Consequently, the Federal Council does not see a need for a fundamental revision of the Anti-Money Laundering Act specifically with regard to cryptobased assets at present.

However, so-called non-custodian wallet providers and certain decentralised trading platforms for cryptobased assets are not subject to the Anti-Money Laundering Act at the moment. The challenges arising in this connection generally have to be addressed internationally within the context of the work of the Financial Action Task Force. Against this backdrop, the Federal Council is currently refraining from proposing that non-custodian wallet providers be subject to the Anti-Money Laundering Act. In contrast, in order to increase clarity for market participants, the current subjection of decentralised trading platforms to the Anti-Money Laundering Act should be anchored more explicitly in law and the possible subjection of other such platforms should be examined in the light of international developments.

Switzerland will continue to play an active role in the competent international bodies to ensure that a globally coordinated and effective mechanism for combating the risks of money laundering and terrorist financing is achieved by means of international standards.

1 Introduction

1.1 Background and objective of the report

Digitalisation is a key driver of innovation, ongoing structural change, and, in the long-term, the competitiveness of the Swiss national economy. Among the remarkable and potentially promising developments in digitalisation is the increasing use of distributed ledger technology (DLT) and blockchain technology. This development is predicted to have significant potential for innovation and efficiency gains in the financial sector as well as other sectors of the economy. In recent years, a remarkable ecosystem with innovative fintech and blockchain companies has developed in Switzerland, especially in the financial sector.

The Federal Council aims to further improve the prerequisites so that Switzerland can make effective use of the opportunities of digitalisation.[1] With regard to DLT and blockchain, the Federal Council believes the best possible framework conditions must be created so that Switzerland can establish and further develop itself as a leading, innovative, and sustainable location for fintech and blockchain companies. At the same time, the Federal Council attaches great importance to ensuring the integrity and good reputation of Switzerland as a financial centre and business location in this area as well. The risks associated with the spread of new technologies should therefore be addressed proactively, and abuses must be combated rigorously.

Against this backdrop, this report analyses selected legal framework conditions in Switzerland with a view to how they facilitate the sustainable development of DLT and blockchain applications on the one hand and how they limit the associated risks on the other. The focus is on applications in the financial sector, where regulatory questions are particularly urgent in light of advanced developments – such as in the frequently discussed areas of cryptocurrencies and initial coin offerings (ICOs).

With this report, the Federal Council is pursuing several objectives:

- Establishing an overview: Firstly, the report is intended to establish a selective overview of the relevant legal framework. It aims not least of all to serve the fintech and blockchain companies themselves, their clients, and the interested public as an information base or reference and to contribute to greater clarity with regard to the applicable legal framework.
- Clarifying the need for action: Secondly, the report is intended to show specifically where, in the view of the Federal Council, there is a need for legal action in the short (and possibly medium) term and where there is currently no need for adjustments. In this way, the report aims to contribute to a better orientation for all stakeholders.
- Achieving signalling effects: Thirdly, the Federal Council is using this report to emphasise that:
  - Switzerland demonstrates openness toward technological developments such as DLT and blockchain;
  - The Swiss legal framework is already as of today suited to deal with business models based on DLT and blockchain;

[1] See e.g. the Federal Council's «Digital Switzerland» strategy of September 2018 with the envisaged goals and guidelines relating to digitalisation and the «Digital Switzerland» action plan, both available at www.bakom.admin.ch > Digital Switzerland and internet > Digital Switzerland (as at 30 October 2018).

- Switzerland wants to further improve its innovation-friendly framework conditions; and
- the Swiss authorities are determined to combat abuses rigorously.

The report also takes up various questions and concerns from parliamentary procedural requests relating to the opportunities and risks of blockchain technology applications for Switzerland. These procedural requests, which demonstrate Parliament's great interest in the subject, include the motions Béglé (17.3818, 16.3484) and Merlini (17.4035), the interpellations Barazzone (18.3272), Müller (17.4144), Noser (17.4213), Schmid (17.4024), and Schneider-Schneiter (16.3272), and the postulate Wermuth (18.3159). The report also addresses the concerns of the postulate "For a competitive financial centre in the field of new financial technologies" (15.4086) of the Economic Affairs and Taxation Committee of the National Council. Finally, the report responds to the concerns raised by the parliamentary initiative Dobler (17.410), which calls for improved protection of data in the event of bankruptcy.

1.2 General comments on the report

While cryptocurrencies such as Bitcoin (also referred to as crypto-based means of payment or virtual means of payment) often attract the most public attention in connection with blockchain/DLT, this report is primarily interested in the underlying technology, which is also the most relevant for future developments. As mentioned in the introduction, it is broadly believed that this technology has great potential to lead to more efficient and resilient processes, for instance in the financial sector, and possibly even disintermediation. How and to what extent this potential will unfold in practice and change the financial sector cannot yet be conclusively assessed. Various scenarios are conceivable in this regard, ranging from individual supplementary applications to fundamental structural changes.

In this context, the Federal Council considers it important for Switzerland to be optimally prepared for all scenarios, including potentially fundamental changes due to DLT. However, in view of technological innovations that are difficult to predict, it is at the same time important not to lose sight of other important developments. Digitalisation in particular involves many other innovations, such as artificial intelligence, big data, cloud computing, the internet of things, mobile applications, and many more, with potentially far-reaching consequences for the economy and society that are not the subject of this report but must be followed just as closely.

1.3 Principles of the Swiss regulatory approach to blockchain and DLT

In the view of the Federal Council, there are several principles that are useful for the future design of the legal framework and the positioning of Switzerland as a location for blockchain companies. The following principles also underlie this report:

- Bottom-up approach: The preferences of the market and society should decide which technologies prevail, while policy should ensure optimal and innovation-friendly framework conditions. In the view of the Federal Council, it is in principle not the authorities' task to decide which technology will prevail and to what extent. This should primarily be up to the market and the preferences of society, along with the technological development itself. It is crucial that the authorities ensure optimal framework conditions that enable the development of new technologies such as blockchain/DLT. If an innovation is technically feasible, offers economic potential, and there are no overriding interests (such as excessive risks) speaking against it, the legal framework should facilitate and support successful implementation. For example, the Swiss legal framework should make it possible to issue and trade shares on a blockchain if this turns out to be beneficial from a technical and economic point of view. The creation of such innovation-friendly framework conditions has a very high priority

for the Federal Council. This also includes the consistent removal of excessive barriers to market entry.

- Targeted adjustments of the well-proven framework: Switzerland should not fundamentally question its proven and balanced legal framework, but should make swift and targeted adjustments if needed where there are gaps or obstacles with regard to DLT/blockchain applications. The Federal Council currently sees no need to fundamentally adjust the Swiss legal framework or introduce a specific new law in response to a specific technology that is still under development. Such an approach might also involve risks, including unclear side effects or a Swiss legislative process that is too slow compared with the technological development. Above all, however, the Swiss legal framework already offers a great deal of flexibility and opportunities. There are nevertheless individual areas of law in which targeted adjustments are needed in order to increase legal certainty, to remove obstacles to DLT/blockchain-based applications, and to limit new risks. This targeted need for action is discussed in this report and should be implemented rapidly.
- Generally technology-neutral approach: Switzerland should continue to pursue a principle-based and technology-neutral legislative and regulatory approach, but allowing exceptions where needed. The rules should be as competitively neutral as possible. The legal framework should not be geared to individual technologies, but rather should treat comparable activities and risks equally in principle, i.e. wherever possible and reasonable. Especially in a rapidly changing technological environment, the development of which can be predicted only to a limited extent by lawmakers, this approach has proved itself. Firstly, it offers a high degree of flexibility. Secondly, it supports the objective of competitive neutrality. Thirdly, a technology-neutral approach alleviates the potential problem that sustainable legislative processes often lag behind technological progress. However, this should not rule out the possibility that there may be exceptional areas in which a specific legal adjustment is called for in regard to distributed ledger or blockchain technology. This may be the case, for example, if existing rules are geared to "analogue" processes and centralised systems instead of digital processes and decentralised systems – and thus are not technology-neutral in their current form. The principle-based approach supports technological neutrality by crafting rules specifying which goal or impact should be achieved, but providing leeway where possible for how to achieve this in detail.
- Legal certainty, clear rules, and combating abuse: Switzerland should position itself as an attractive location for blockchain companies through legal certainty, efficient regulation, and a good reputation. Fraudulent or abusive behaviour as well as the use of innovative technologies to circumvent financial market regulation will not be tolerated. Innovation-friendly framework conditions should not be confused with a rule-free environment. Instead, legal certainty also goes hand in hand with the consistent application of relevant rules. If a new technology wants to assert itself on the market sustainably and successfully, it must create added value in the longer term under comparable rules and in competition with existing solutions. This added value may for instance be higher transparency, resilience, or efficiency. Conversely, it would hardly be in the interests of overall economic efficiency if a technology were to prevail over another solely because it is not subject to comparable regulatory requirements. It is undoubtedly also in the interest of the still young blockchain industry if it can adapt early on to clear legal requirements and if it can move from the pioneer phase into a phase of broader, sustainable market penetration in a business location characterised by legal certainty, a good reputation, and a confidence-building environment.

– Openness and dialogue: Swiss authorities should position themselves as open towards new technologies and innovations such as blockchain and DLT and cultivate regular dialogue with the industry. Innovation-friendly framework conditions are determined not only by regulatory requirements, but also by the openness of the competent authorities to new technologies – such as blockchain and DLT – and by the accessibility of these authorities for market participants. Not least of all with a view to the rapid development of blockchain/DLT technologies, Swiss authorities are deliberately positioning themselves as open and are cultivating an active and regular dialogue with the industry at all levels.

1.4 Development and structure of the report

The report is based on the analyses and work of the blockchain/ICO working group established by the Federal Department of Finance (FDF) in January 2018.[2] The creation of this working group was announced in the Federal Council's response of 15 November 2017 to the Béglé motion (17.3818). The focus of the report is on selected legal aspects under civil law, the requirements under financial market law, and the legal provisions for combating money laundering and terrorist financing, as well as on the consequences of this legal framework for all DLT and blockchain business models in the financial sector.

As part of its analyses, the working group composed of members of federal authorities[3] conducted broad exchanges with the private sector. On the basis of a consultation paper,[4] it conducted an informal consultation with the fintech and financial industry on various aspects in September 2018. The evaluation of this consultation was incorporated into the conclusions and will be taken into account in the suggested follow-up work. Supplementing the written submissions, feedback on this consultation was also given in a round table with representatives of the fintech and financial industry chaired by Federal Councillor Ueli Maurer. The preparation of this report also took into account the recommendations of the white paper of the "Blockchain Taskforce", a private industry initiative, published in April 2018.[5] Exchanges were also conducted with this task force. Additionally, members of the working group held numerous discussions with individual representatives of the fintech and financial sector, law firms, and business associations.

The report first presents the fundamentals of distributed ledger and blockchain technologies (section 2) and then looks at various applications in the financial sector (section 3). After a brief description of the international context (section 4), section 5 discusses the basis under civil law – in particular the classification of tokens and their transfer under civil law – as well as the treatment of tokens in insolvency proceedings. Tokens are then examined from the perspective of financial market law (section 6) and combating money laundering and terrorist financing (section 7). Section 8 contains a brief summary of the responses received in the consultation procedure.

1.5 Other relevant framework conditions

In addition to the aspects under civil and financial market law discussed in the report, other framework conditions are also decisive for the future development of fintech and blockchain companies in Switzerland. The aspects briefly outlined below are not discussed in detail in this report for various reasons, either because separate work has already been done or is planned

---

2 See FDF press release of 18 January 2018, available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-69539.html (as at 18 October 2018).

3 With representatives of SIF, FOJ, FINMA, SNB, fedpol, FCA, and SECO.

4 See the consultation document available at: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-72001.html (as at 18 October 2018).

5 See Blockchain Taskforce 2018a.

on these aspects, because these aspects are not directly part of the legal framework, or because their treatment would have exceeded the scope of the report.

Tax environment

Activities based on DLT and blockchain raise a number of questions that have to be clarified regarding their tax status, given that the new technology is transforming business models. In particular, issues relating to value added tax, stamp duties, withholding tax, profit tax, income tax, and wealth tax require in-depth analysis to be carried out by the FDF in 2019. In the view of the Federal Council, the further development of the fintech and blockchain ecosystem in Switzerland depends on an attractive tax framework that also ensures legal certainty and predictability. In principle, a technology-neutral approach should also be pursued in the area of taxation.

Electronic identification (E-ID)

Another key element for the further development of digital business models, whether for typical online business or for DLT-based activities, is the creation of a state-recognized electronic identity, also called E-ID. The E-ID confirms the existence and identity of a natural person on the basis of unique personal identification data contained in state-run registers. This creates a high level of trust and security in the online sector, both for consumers and for providers of online services. Several alternatives are envisaged as carriers for the E-ID, and a technologically neutral formulation was deliberately chosen in order to do justice to future developments as well. E-ID will be issued in collaboration between public and private actors. The dispatch on the E-ID Act was adopted by the Federal Council on 1 June 2018.[6] The proposal is now being considered by the Swiss Parliament. The E-ID Act is expected to enter into force at the beginning of 2021.[7]

Access to bank accounts

Another essential prerequisite for the successful development of fintech and blockchain companies – as is the case for all start-up companies – is access to bank accounts. At least so far, the opening of bank accounts for blockchain companies has been a challenge in practice for several reasons both for these start-ups and for the banks. This has been observed not only in Switzerland, but also in other countries. The problem is known to the industry and the authorities. But it cannot be solved directly by legal means unless a legal right to a bank account were to be created, which would raise new and difficult questions and is not considered a reasonable solution. The FDF instead convened a round table in the summer of 2018, and the Swiss Bankers Association has meanwhile dealt with the issue extensively in a working group involving the *Crypto Valley Association*. As a result, the Swiss Bankers Association has developed guidelines published on 30 September 2018 that are intended to assist banks in opening bank accounts for blockchain companies.[8] The goal must now be for both blockchain companies and banks to further strengthen their cooperation and promote mutual understanding of the existing concerns and framework conditions.

Data protection

Another important topic in the DLT/blockchain context is data protection. For instance, facts can be made permanently reproduceable and traceable using DLT and blockchain, which

---

6 Dispatch of 1 June 2018 on the Federal Act on Electronic Identification Services, in: BBl **2018** 3915.

7 See «Digital Switzerland» action plan of 5 September 2018, 17, available (in German, French, and Italian) at www.bakom.admin.ch > Digital Switzerland and internet > Digital Switzerland (as at 18 October 2018).

8 See guidelines of the Swiss Bankers Association (SBA) of September 2018 on opening corporate accounts for blockchain companies. Available at www.swissbanking.org > Media > Positions and press releases (as at 18 October 2018).

raises data protection questions. While this report does not discuss these questions in detail, an interdisciplinary group of experts appointed by the Federal Council on the future of data processing and data security has already dealt with issues including blockchain and data protection. The Federal Council adopted this report on 10 September 2018 and has mandated the Federal Department of the Environment, Transport, Energy and Communications (DETEC) to analyse the recommendations of the report and to clarify further steps in consultation with the departments concerned by mid-2019.[9]

e-franc

The present report also excludes the question of the creation of digital central bank money or "e-franc". However, in response to the Wermuth postulate (18.3159) adopted by the National Council, the FDF will prepare a separate report on the opportunities and risks of introducing a crypto franc (e-franc), which is expected to be available by the end of 2019.

Other framework conditions

In addition, there are other general location factors that are relevant for fintech and blockchain companies – as well as for most other companies – and that are not discussed in detail in this report. These include the training and availability of a qualified workforce, market access for service providers to other jurisdictions and in particular to the European Union, political and economic stability, the general infrastructure, and quality of life in Switzerland.

9 See report of the expert group on the future of data processing and data security of 17 August 2018. Available (in German, French, and Italian) at www.efd.admin.ch > Documentation > Press releases > Press release of 10 September 2018 (as at 18 October 2018).

2 Fundamentals of DLT/blockchain

2.1 Introduction

With the implementation of Bitcoin at the beginning of 2009, something new was created: Bitcoin makes it possible for participants who do not trust each other and who do not know how many other participants are in the system to maintain a shared accounting dataset. The technology that makes this possible is called blockchain, and it provides the basis for a new data management model. The term "blockchain" refers to the grouping of transactions into blocks, which are then jointly validated. This validation in turn attaches the block with the new transactions to a chain of previous blocks and thus incrementally builds up a transaction history.

The basic functioning of the blockchain corresponds to the model of the replicated state machine, i.e. a system in which participants manage a volume of data (state) by holding a copy of the data (replica) locally and performing operations on it that modify the data. It is important in this regard that the initial state is the same for all participants and that the operations are deterministic. Deterministic means that any participant who applies the operations to the initial state in the same order will arrive at exactly the same result. In this kind of system, "consensus" means that all participants agree on the current state of the data. In the case of Bitcoin, the data are the Bitcoin balances of the individual participants, and the operations are the transactions between these participants.

The abstract functionality of shared data management is potentially very useful in many areas, and attempts are being made to solve many problems with blockchain and other consensus mechanisms. Some applications are based closely on the example of Bitcoin, with blockchains accessible and visible to everyone, while others are based on consensus mechanisms derived from research in distributed computing and distributed systems (formal consensus and Byzantine agreement).

The diversity of the systems based on these approaches goes beyond blockchain as such, which is why the broader term distributed ledger technology (DLT) has been introduced. In this report, DLT refers to technologies that allow individual participants (nodes) within a system to securely propose, validate, and store operations in a synchronised dataset (ledger) that is distributed across all nodes in the system. Blockchain is a possible form of how data can be stored in such a system: operations (e.g. transactions) are grouped in a block, and this block is attached to the last previously created block. This allows operations and data to be stored without allowing them to be subsequently modified.[10]

2.2 Fundamentals of DLT using the example of Bitcoin

The original version of Bitcoin was set out in an article by Satoshi Nakamoto published in 2008[11] and has been steadily developed as an open source project ever since. Bitcoin can be considered a type of digital cash that enables electronic payments between two parties without the need for a third party to maintain a record of the transaction. Bitcoin combines achievements from the fields of cryptography and distributed systems. The key elements are briefly presented below and then brought together to explain the Bitcoin blockchain.

---

10 On the fundamentals of cryptography, see section 2.2.
11 Nakamoto 2008.

Cryptographic hash functions

For an input value of any given length (input), a cryptographic hash function returns a fixed-length string of characters (hash) as the output value (output). Two important properties of a cryptographic hash function are:[12]

- One-way function: The hash function cannot be used to deduce the original input from the hash;
- Collision resistance: It is virtually impossible for two different inputs to generate the same hash.

Digital signatures

For digital documents, a digital signature should in principle reproduce the properties of physical signatures on paper. To do this, it must exhibit two characteristics:

- Only the signing person can sign, but any other person can validate the signature.
- The signature is valid for a specific document and cannot be applied to other documents without the consent of the signatory.

In principle, a digital signature is a sequence of bits generated by the sender using a signature scheme[13] for a message. Typically, this signature is appended to the message and sent along with it so that the recipient can verify that the message actually originated with the sender and was not modified during transmission.[14] A digital signature scheme makes it possible to:

- Generate a pair of keys consisting of a signing key (private key) to sign messages and a verification key (public key) to verify signatures. The private key must be kept secret, while the public key is typically made public.
- Generate a signature for a given message with a given private key.
- Verify the validity of a given signed message using a given public key.

Public keys as identities

Public keys (or addresses) correspond to identities of Bitcoin users. Bitcoin users can send a message (i.e. transaction) from their address by signing the transaction with their private key. Bitcoin has no central authority that registers or identifies users. All users register themselves by generating – as often as they want – a new address. At first glance, this decentralised identity management gives the impression of granting users a high degree of anonymity and privacy. But this impression does not entirely hold up over time. Movements are attributable to each address which are visible to all participants and behind which patterns can be recognised. This is why Bitcoin is often referred to as a pseudonymous system.[15]

Transactions

The elements presented above can be used to represent the structure of a Bitcoin transaction (see figure 1). Alice (Owner 1) sends a token[16] to Bob (Owner 2) to by signing the hash of the

---

12 For a detailed discussion of cryptographic *hash* functions in cryptocurrencies, see e.g. Narayan/Bonneau/Felten/Miller/Goldfeder 2016.

13 Bitcoin makes use of the *Elliptic Curve Digital Signature Algorithm* (ECDSA) developed by the US government.

14 Brünnler 2018: 4.

15 See also section 2.3.5.

16 More precisely, a transaction consists of *inputs* and *outputs*. An *output* is essentially the sum of what the payee can spend as a result of this transaction. An *input* is a reference to the *output* of a previous transaction. If Alice has 5 tokens and wants to transfer them to Bob, she creates a transaction with one *input* and one *output*. The *input* references her 5 tokens. The *output* contains the number 5 and Bob's *public key*. If Bob now wants to

previous transaction and Bob's public key. Bob can verify the signature and thus the previous ownership. This assures Bob that the message has been signed by Alice and has not been falsified. A token is understood to be a piece of information stored on a blockchain. (The terms "coin" and "token" can often be used synonymously).

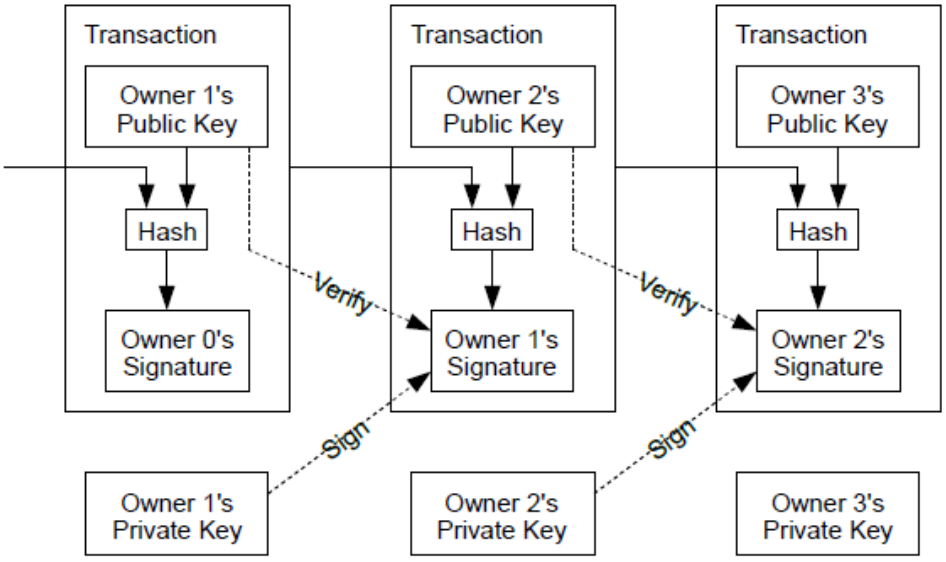

Figure 1 Bitcoin transaction (Satoshi 2008)

This does not yet address the problem of double-spending: Bob does not know whether Alice has already sent the token to someone else. In a decentralised system, this problem can be solved only if all transactions are known and all participants agree on their chronological order. This requires additional elements:

Blockchain

A blockchain is a data structure in which the data is stored in individual linked blocks. The linking of the individual blocks is done with a hash pointer. The hash pointer contains the information where certain data is stored, and it also contains a hash of this data (see figure 2). If the data of a block is changed, the hash of this block also changes. The blockchain is therefore a possible form of a ledger in which data is stored.

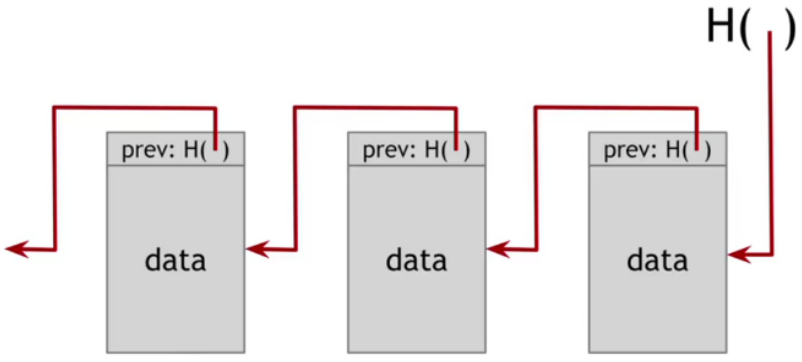

Figure 2 Blockchain with hash pointers

use these 5 tokens to buy a coffee worth only 3 tokens from Charlie, he creates a transaction with one *input* and two *outputs*. The *input* references the *output* of Alice's transaction. The first *output* contains the number 3 and Charlie's *public key*. The second *output* contains the number 2 and Bob's own *public key*, so that he transfers 2 of the transferred 5 tokens to himself. Analogously, there is a transaction with two *inputs* and one *output* if Charlie has received 2 tokens and 3 tokens from different sources and now wants to transfer 5 to Dave (see Brünnler 2018: 38).

Digital timestamp

Digital timestamps serve to prove the existence of certain data at a certain point in time. In the case of Bitcoin, a timestamp is added to the hash of a block content. This proves that the block content existed at a certain point in time.

Proof-of-work consensus mechanism

The Bitcoin system is designed to ensure that participants can reach a consensus among themselves on the ledger without a central body performing this role. This consensus ultimately gives rise to the determination of who owns how many Bitcoins. This also is considered the principle of truth in the case of Bitcoin: the allocation of a Bitcoin is nothing more than the fact that the nodes agree to whom that Bitcoin is allocated.[17]

Reaching consensus in a decentralised system is a major challenge. In the case of Bitcoin, various transactions are sent to the network by the users, and the individual nodes must reach consensus on which transactions took place in which order. Only if all nodes can agree on a certain set of transactions (combined in a block) can the double-spending problem be solved. The consensus mechanism is triggered when transactions can be brought together to create a block.

Bitcoin uses the proof-of-work mechanism to reach consensus. Under this mechanism, (substantial) computing power is used to execute cryptographic functions until the result exhibits certain properties. If the desired property is fulfilled, this is considered valid proof-of-work. The cryptographic function makes it impossible to check the validity of the proof-of-work without actually executing the function. But with a valid input, it is trivial to check validity. This forces the participant to guess a valid input by repeatedly trying out alternatives (work). Bitcoin uses a one-way function (specifically a SHA-256 hash function[18]) until the output has a certain prefix (specifically several 0 digits).

Bitcoin network

The Bitcoin network is a peer-to-peer network consisting of many equal nodes. Anyone can operate a node by installing Bitcoin client software on their computer. The purpose of the network is to manage the blockchain. This ensures that all transactions are validated (correct form, no double-spending) and distributed to all nodes. The same occurs with newly created blocks, where validation consists in verification of the hash for the created block, verification of all transactions contained in the block, and assurance that the block has been added to the longest chain[19] of the blockchain.

Functioning of Bitcoin

These elements can be used to describe the decentralised character and functioning of Bitcoin:

Anyone wanting to send or receive Bitcoin does not have to reveal their identity but rather must create a pseudonymous address and the corresponding private key. The instructions for the transfer of Bitcoins (i.e. for a specific transaction) between different addresses are then sent to the peer-to-peer network in the form of a message. The network aims to ensure that all messages are distributed to all participating nodes. The transactions contained in the messages must be validated by the network (see above). Miners (the validating nodes) combine transactions into a block for this purpose and try to achieve the proof-of-work as quickly as possible and send it to the network for verification. The nodes accept a block only if

---

17 Narayan/Bonneau/Felten/Miller/Goldfeder 2016: 47.

18 SHA stands for Secure Hash Algorithm, developed by the US National Security Agency (NSA).

19 By definition, the longest chain is always the one with the most cumulative computing power. Otherwise, it would be relatively easy to create a longer chain with lower *difficulty* (i.e. less cumulative computing power).

the transactions it contains are valid. If this is the case, the miners begin work on the creation of the next block. Miners are compensated with newly created Bitcoins and transaction fees.

Nodes always consider the longest chain[20] of continuous blocks to be the correct one. The irrevocability of a transaction thus becomes more probable with each attached block, but the transaction is never considered definitive under this probabilistic approach.

Forks

The Bitcoin protocol is being further developed on an ongoing basis.[21] A new version of the protocol must be adopted and implemented by the nodes in the network. In practice, this is a difficult undertaking, given that it is not possible to force the nodes to change the protocol. This means that the nodes have different versions of the protocol, which – depending on the change – can have different consequences.[22]

If the change affects the rules in such a way that blocks are validated that would not have been validated in the previous version (e.g. larger blocks), this is deemed a hard fork. This creates a chain of blocks with the new properties which is then further developed by the nodes with the new protocol. Because these blocks are considered invalid by the other nodes, there are now two parallel transaction histories with a common prehistory: one without the change, the other with the change. The two chains are incompatible and no longer interoperable.

If a change makes the validation rules more rigorous, this means that the new protocol will cause nodes to reject some of the blocks accepted by the old nodes. If the majority of the nodes operate with the new protocol, the new rules will prevail. Miners using the old protocol will find that some of their proposed blocks will be rejected and that they will not receive compensation for them. If they do not want to accept these losses, they will adopt the new protocol as well. This prevents permanent separation of a chain of blocks and is referred to as a soft fork.

2.3 Design of a DLT systems

Over time, different versions of DLT have developed, which can be distinguished according to different dimensions. What they all have in common is the shared management of data and the modification thereof through operations applied to that data. Some of these dimensions constituting essential properties of a DLT system are explored below. An important element in the development of a new system is to make a choice for each of these dimensions.

2.3.1 Application and flexibility

The design of an application based on a DLT system defines the data model to be jointly managed and the operations that can be applied to it. One can define the application very narrowly or very flexibly. In general, a narrower application is easier to optimise, while a more flexible application incurs higher costs (more difficult protocol, less predictability, larger target for attacks, etc.).

Bitcoin is a very narrow application. The managed dataset consists of transactions and the resulting balances (tokens) allocated to specific addresses. The operations applied to that dataset are transactions that assign tokens to new addresses. Operations can access only tokens and their metadata that is modified by the transaction. It is not possible to access the data arbitrarily, but rather the transactions act in isolation from each other.

---

20 Narayan/Bonneau/Felten/Miller/Goldfeder 2016: 47.

21 In principle, the development of Bitcoin is *open source*, i.e. anyone can propose changes to the protocol. The driving force is a group of about 100 programmers (Bitcoin Core).

22 Narayan/Bonneau/Felten/Miller/Goldfeder 2016: 73 et seq.

Ethereum is the counterexample, namely a very flexible application. The operations are described in a more powerful (Turing-complete) language, which can also access data written by previous operations. This makes it possible to store any kind of data on the blockchain and modify it later. But this flexibility also means that it is considerably more difficult to optimise: for example, the computational effort required to perform an operation cannot be estimated (halting problem).

There are numerous variants between the two extremes of Bitcoin and Ethereum. For example, the actual execution of operations can be outsourced, so that only the final values are processed with proof of execution by the nodes. This is in particular the case with so-called zero knowledge systems, where the participants see only the changes to the data, but not the operations performed.

In addition to pure data, it is also possible to store program code on blockchains. This code is then launched by operations and carries out predetermined calculations. These programs are also called smart contracts. Various people can interact with each other through a smart contract even where they do not trust each other. This means a smart contract can assume the role of a central mediator.

A decentralised autonomous organisation (DAO) is an example of a smart contract in which the smart contract can autonomously dispose of the resources of an organisation. The governance of the organisation is described in the smart contract, guaranteeing that the organisation behaves as described. In 2016, "The DAO" was created as an investment fund with the aim of jointly managing it. The DAO's software code had a bug, however, allowing an attacker to steal USD 50 million worth of money.[23]

Another form of smart contract are DApps (decentralised applications such as a game, an exchange, or the like), which are executed in whole or in part on the blockchain. In all these examples, the added value is that the behaviour is defined from the outset and that all participants who interact with the smart contract can rely on the fact that the smart contract is behaving correctly.

Not only the transfer of Bitcoins can be registered on the blockchain, but also the transfer of other data. For this purpose, the Bitcoin protocol is supplemented by an application-specific programmed protocol. The blockchain serves as a basis and guarantor for the security of the application. The attached protocol makes it possible to include additional metadata on the Bitcoin and store it as part of a transaction, such as the information "Negotiable Security X". The attached information can be thought of as the 'colouring' of a Bitcoin, which is why these applications are often referred to as coloured coin models. By using blockchain transactions to perform a technical transfer of metadata relating to assets from one person to another, such as negotiable securities, the model can be used to register the ownership of assets on the blockchain without the need for a central register. An important difference to Bitcoin in this model is the reference to an external asset.

2.3.2 Access

The terms *permissioned* or *permissionless* are often used in reference to DLT systems (see table 1).

Permissioned DLT systems have restricted access and are primarily operated by consortia. The participants know each other, and the number of participants in the system is also known.

Permissionless DLT systems are systems in which the participants can join or leave at any time, and no central authority grants access. This means that in such a system, it is not clear

[23] For details on DAOs, see the discussion in section 6.7.2.6.

how many participants are in the system at a given time. Consequently, classical consensus algorithms based on voting are not applicable, because the number of votes required for a majority is unknown.

The terms permissioned and permissionless can also refer to the write permissions in the system, i.e. which participants are authorised to validate operations. It must also be specified who has read access to the data. In the case of a permissionless DLT system, in principle every participant has read access, given that every participant can also participate in the consensus, for which read access is a prerequisite. In a permissioned DLT system, on the other hand, the data may be publicly accessible or accessible only to certain auditors and consensus participants (in this case validators).

Table 1: Systems with different degrees of centralisation (Source: CPMI 2017: 8)

Description	Existing systems of the centralised financial market infrastructure	Only approved entities can use the service. Roles are differentiated.	Any entity can access the system and play any role.
Validation	Centralised validation	Decentralised validation	
Access	Restricted		Unrestricted
Roles of participants	Differentiated		Not differentiated
Example	SIC payment system	Corda, USC	Bitcoin, Ethereum

2.3.3 Consensus mechanism

A characteristic shared by all DLT systems is that a large number of participants – who trust each other only to a limited extent – have to agree on the current state of the system. There are several ways to achieve this consensus. For this purpose, consensus algorithms establish a shared sequence of operations to verify validity and to achieve a shared final state.

In the case of permissioned DLT systems, i.e. systems with access control, it is possible to use classical consensus algorithms from the field of distributed computing, such as Paxos or Practical Byzantine Fault Tolerance (PBFT). Under these protocols, participants vote on the next operation to be performed. This is possible because each participant knows how many votes constitute a majority and when the vote is successful.

In the case of permissionless DLT systems, which do not have access control, this type of voting is not possible, given that each participant can pose as any number of independent participants (Sybil attack) and a vote can never be completed. These systems therefore need a mechanism that makes it unattractive for participants to work against the system. For this purpose, a participant is randomly selected to propose the next operation to be performed. The other participants can accept this proposal by building on it if they are selected next. Individual operations are grouped into blocks in order to increase the efficiency of the system.

Bitcoin uses the proof-of-work mechanism for this purpose, in which cryptographic functions are executed until the result has certain properties.[24] In a proof-of-work system, the probability

[24] See section 2.2.

that a participant finds the next valid block depends solely on the participant's processing power. Specialised miners therefore maintain large computing capacities, leading to high energy consumption of the proof-of-work systems. For a miner, it makes economic sense to operate this computing power as long as the costs are lower than the expected income from successfully validated blocks.

As an alternative to proof-of-work, there is for instance the possibility to select a random participant on the basis of the data in the system. In the case of crypto assets, for example, a (pseudo-)random token can be selected whose assigned address (stakeholder) can make the next proposal for the further development of the blockchain. In such a proof-of-stake system, the probability of being permitted to make the next proposal increases with the participant's tokens. This eliminates the need for time- and energy-consuming proof-of-work calculations, and participants with a greater interest in the continued existence of the system (because they have invested in it) make the decisions relatively frequently. However, implementation of this concept is not easy, given that participants are able to act strategically, thus increasing their influence in the system, or act incorrectly. So far, most proof-of-stake systems have therefore used a combination of proof-of-stake and proof-of-work to address these manipulation attempts, but they accordingly still have the disadvantage of high energy consumption.

2.3.4 Log structure

The sequence of all operations applied in a system is also called a *log*. In the case of blockchains, the operations are grouped into blocks and arranged in a linear list (chain). Apart from such a linear list, however, other structures can also be used for the log, provided that the order of execution is always clear for operations that might be mutually exclusive. For example, a tangle creates a partial order. Using this method, transactions also validate earlier transactions, so that the transactions concerned are ordered among themselves. Hybrid forms are also possible: while Ethereum has a linear blockchain, it can reunite branches that occur naturally ("uncle blocks").

In the case of permissioned DLTs, the log can be dispensed with, since the participants who specify the ordering of operations are completely trusted. Unlike in the case of permissionless DLTs, a newly joining participant does not have to recalculate all operations starting with the initial state, but rather takes over the current state from an existing participant and then builds on it.

2.3.5 Anonymity and privacy

Pseudonymity for Bitcoin

In the case of Bitcoin, stakeholders do not need to use their real name, but their addresses serve as their identity within the system. This intermediate form is often referred to as pseudonymity.[25]

Users can manage their anonymity to a certain extent through their own behaviour. They can create new addresses as often as they want. However, this is able to increase anonymity only if addresses created by the same user cannot be associated with each other. As soon as transactions are performed, the probability increases that patterns and connections between addresses controlled by a single user will be recognised.

Other ways to increase anonymity are mixers and certain wallet providers. With a mixer, users can send tokens along with information about the desired recipient to the address of the mixer. The mixer then sends (other) tokens from that address to the address specified by the user. A similar mixing of tokens can also be achieved via wallet providers that combine the tokens of

[25] See section 2.2.

all users in a pool. When using mixers and these kinds of wallet, anonymity is increased only if no information about the users is recorded.

In general, it is difficult for Bitcoin users to achieve complete anonymity, given that every Bitcoin transaction is recorded and stored, and patterns and connections become recognisable as the transaction history increases.

Anonymity in other crypto-based systems

Both businesses and individuals may have an interest that not all their data can be inspected by neighbours, co-workers, business competitors, etc. in an open blockchain. Developers of various crypto-based systems therefore endeavour to increase the anonymity of their users compared to Bitcoin. Various technological possibilities are available for this purpose, which for instance attempt to conceal (e.g. Monero) or interrupt (e.g. Zerocoin) the traceability of transactions.

2.3.6 Scaling

Currently, all participants in Bitcoin and many other blockchains store a large amount of data (namely the entire transaction history) and process each individual transaction. This leads to a high level of resilience of the system but impairs its scalability. This problem is addressed by software developers by splitting the data volume and operations into groups (sharding) or by reducing the load on the network by aggregating many small operations (off-chain protocols).

Sharding divides the participants, the data, and the operations into groups (shards). Participants within a group process transactions only within that group, so that they have to store less data and process fewer operations. Participants no longer validate all operations in the system; instead, participants in a group validate only group-specific operations. This means the rate of executable operations increases linearly with the number of shards. However, the work involved in a cross-group operation also increases, which happens more frequently as the number of groups rises. An example of sharding is the Plasma protocol, with which the Ethereum blockchain can be divided into several small, mutually independent blockchains, thereby distributing the workload.

Off-chain protocols, such as the Lightning Network for Bitcoin or state channels for Ethereum, aggregate numerous off-chain operations – which are negotiated among a small group – into a few on-chain operations. In the Lightning Network, for instance, two endpoints open a payment channel for a certain credit balance. This credit balance can then change owners any number of times, and only at the end of the channel are the credit balances paid out to the end points through a blockchain transaction. This distributes the on-chain costs across any number of off-chain transactions.

While on-chain transactions can be time-consuming because they require confirmation by the blockchain participants to be valid, off-chain transactions can in principle always be carried out immediately, with no validations taking place on the blockchain. Instead, the parameters for the validity of an off-chain transaction are formulated in the rules and technical standards of the off-chain system or determined autonomously by the operators of such systems.

2.4 Stakeholders in the DLT world

Various economic operators and stakeholders in the world of DLT are described below, along with their functions. For a discussion of these activities and stakeholders under financial market law, see the comments in sections 6 and 7.

Mining companies

Miners are validating nodes; they are relevant to blockchain models that allow the mining of tokens in proof-of-work blockchains (to be distinguished from "pre-mined tokens"). In Switzerland, companies specialising in mining are less numerous and significant than in other countries.

Wallet application developers

Developers of software providing a user interface to manage tokens. In general, a distinction can be made between providers of non-custodian wallets and custodian wallets. The former are typically decentralised open source projects that cannot necessarily be attributed to individual companies. Their software applications are often provided free of charge (freeware). These wallets allow users to create their own key pairs (i.e. private key and public key), which means the developer has neither knowledge of nor access to the generated key pairs of the users, given the lack of a customer relationship or proximity. Providers of custodian wallets, on the other hand, often maintain a long-term customer relationship and manage the key pairs for this purpose (see also custody services).

Crypto brokers & exchanges

Companies active in the secondary trading of tokens already in circulation. As exchanges, these companies may either serve directly as counterparties (two-party relationship), or they may buy and sell tokens on behalf of the customer. A distinction can be made in this regard between crypto-to-fiat transactions and crypto-to-crypto transactions. The latter are carried out directly via the blockchain or via off-chain solutions linked to the blockchain.

In Switzerland, several providers are currently operating in this field. Occasionally, traditional participants in the financial market (e.g. asset managers and banks) also offer services for this purpose.

Crypto trading platforms

Companies that are active in the secondary trading of tokens that are already in circulation. As trading venues and in contrast to exchanges, they maintain an order book and bring their market participants together by matching supply and demand (three-party or multi-party relationship). A distinction can be made in principle between two types of trading platforms:

Centralised trading platforms use their own cryptographic addresses or wallets to maintain credit balances for their customers. They have a special role to play within the crypto ecosystem, given that they are the main venue for the conversion of conventional currencies (e.g. CHF, USD, GBP, etc.) into cryptocurrencies. For this reason, most of these platforms also offer their own bank accounts for customers to maintain balances in conventional currencies (e.g. Bitstamp, Coinbase, Kraken).

In the case of decentralised trading platforms, the token credit balances are in principle located at the blockchain addresses of the users' themselves. Here again, supply and demand are matched by the trading platform. The tokens are typically transferred in advance to a smart contract, which holds them until the order – placed on a virtual trading floor, for example – can be processed; as is the case with a conventional blockchain transaction, the user generally has to provide a cryptographic signature for the transaction. The decentralised nature of such trading platforms refers less to the trading platforms themselves than to the downstream settlement, which takes place directly between the parties (peer-to-peer).

So far, secondary trading via crypto trading platforms (both centralised and decentralised) has mainly taken place outside Switzerland.

Custody services

While blockchain users may keep their tokens on their own devices and wallet addresses at any time, they may regularly also have the need – for reasons of security – to store their tokens with specialised providers that offer enhanced technical protection measures. For this purpose, the tokens are located on specialised infrastructures that are either managed online ("hot storage") or are separated from the internet and thus should offer enhanced protection against hacking attacks or other interference ("cold storage"). These providers include specialised companies offering custody services as a core activity ("crypto custodians"), but secure technical storage of assets is also increasingly being offered as an ancillary service by other market participants (in particular crypto trading platforms and brokers).

Custody services are currently offered in Switzerland both by pure crypto custodians as well as by other blockchain service providers.

Peripheral blockchain services

In connection with the increase in initial coin offerings (ICOs), new services are emerging at the periphery that aim to support and accompany such ICOs. These services are generally not provided on the blockchain. Examples include the provision of forensic analysis tools, know-your-customer (KYC) software, and tools for transaction monitoring.

Developers of blockchain protocols / issuers of blockchain-based tokens

Blockchain technology is often used for issuing new tokens, which can be done in two ways: firstly, tokens can be programmed directly into the architecture as part of the creation of a new blockchain protocol ("native" or "intrinsic" tokens, [see section 3.2]). In these cases, the tokens often have the function of a network resource. Currently more widespread is the use of certain existing blockchain architectures (especially the Ethereum blockchain) for the purpose of issuing new tokens by their users. This is generally done as an ICO.[26] These tokens are based on uniform technical standards, but to a large extent they can be designed freely by the issuer in terms of their intended purpose.

In both versions, the programming teams – which often have a decentralised organisation – play an important role. These teams are often also involved in the further development of existing open source protocols.

2.5 Technological obstacles

2.5.1 Possible design trade-offs

The discussion in section 2.3 entails that DLT systems can be designed differently along certain dimensions, for example with regard to access (open or restricted), scalability, and anonymity of the participants in the system.

The demands on the design of a DLT system depend on the intended application (see also section 3). Some applications are based on high throughput for transactions and thus require corresponding scalability. This is the case, for example, in retail payment transactions, where thousands of transactions have to be processed per second. Other applications need to guarantee a high degree of privacy (e.g. administration of patient data), or their systems need to be particularly resistant to data loss, loss of integrity, lack of availability, or manipulation (e.g. voting and elections, administration of land registers).

Different designs of DLT systems along these dimensions result in certain trade-offs (see figure 3). For instance, the availability of the system increases, the larger the number of validating

[26] See section 2.2.

nodes is. At the same time, however, throughput decreases with the number of fully validating nodes. Resilience against data loss also increases the sooner the full dataset is replicated on all nodes. At the same time, however, confidentiality is reduced as information is shared. In the Bitcoin network, for example, all information provided for in the protocol is fully replicated. While a certain degree of confidentiality can be achieved by encryption even when the data is universally distributed, this makes it more difficult to gain insights into the integrity of the data. And in turn, throughput may decrease for certain applications.

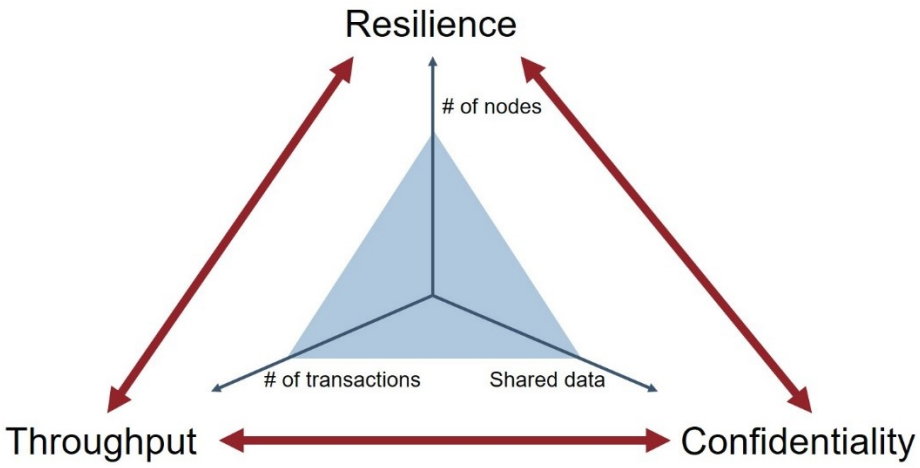

Figure 3: Trade-offs in the design of a blockchain (own illustration, based on Bank of England[27])

Thanks to ongoing research, it is possible that these trade-offs and the associated limits will change in the future. For example, new protocols might keep throughput high even with a larger number of validating nodes. Encryption technologies (e.g. obfuscation, zero knowledge proofs) make it possible to distribute data with encryption, thus resulting in a lower reduction of confidentiality. Due to physical limits (e.g. latency when updating the network state), these trade-offs will continue to be the subject of future decisions regarding the design of a blockchain.

In principle, reaching consensus among a large number of participants in a system who do not know each other and do not trust each other is a challenging task, setting limits on the scalability and information security of the system. This must be kept in mind for applications in certain business areas, such as the financial sector.

2.5.2 Operational risks

Operational risks are risks which – due to errors in the technology infrastructure[28] or internal processes, human error, or external events – lead to the reduction, worsening, or outage of the services provided on a system or network. Possible operational problems include disruptions or delays in processing, system outages, insufficient system capacity, fraud, and data loss.[29]

The following discussion primarily focuses on operational risks that may newly arise or become more serious due to the application of DLT. It therefore does not consider all the possible risks that might also exist for other electronic infrastructures (e.g. power outages).

---

27 Scorer 2017.

28 «Technology infrastructure» refers to the physical and logical (electronic) design of IT and communication systems, the individual hardware and software components, the data, and the operating environment.

29 CPMI/IOSCO 2012: Principle 16.

Availability and integrity

Decentralised validation and the distribution of data among a large number of nodes can alleviate the problem of the single point of failure and in principle increase the availability of the overall network. However, distribution among many nodes also creates more potential gateways for attacks against the network. The integrity of the overall network thus largely depends on the security standards of the individual nodes: if the security requirements for the individual nodes are low, even a decentralised network with a large number of validating nodes may be insecure overall. Although the distribution of the information increases the availability of the overall network in principle, resilience also substantially depends on the integrity of individual nodes.

The consensus mechanism also plays a key role in the reliable functioning of a decentralised system. The crucial factor in this regard is how large the failure tolerance of the consensus mechanism is or under what conditions a system state is accepted as certain. These requirements vary depending on the consensus mechanism. If the requirements for the consensus mechanism are too rigid (e.g. unanimity among all nodes), it may not be possible to achieve a consistent state, and the system may not be available (CAP theorem).[30] If, on the other hand, the requirements are not strong enough, agreement may be reached, but the integrity of the system can more easily be compromised by malicious nodes.

Encryption technology

Cryptographic algorithms, in particular asymmetric cryptography (public/private key cryptography) and cryptographic hash functions (see section 2.2) are critical elements for the secure functioning of a DLT system. While these cryptographic algorithms meet current security requirements – and are in fact also used beyond DLT in other areas of digital communication such as email and https – it is certainly possible that future technological developments (e.g. in the field of quantum computers) may make adjustments necessary. In this context, it is important for the governance of a DLT system to take technological advances into account, so that, for example, encryption technology can be adapted as needed (on governance, see also below).

Data management and data protection

Confidentiality: In principle, the confidentiality of data decreases as it is distributed among more nodes in a system. From the standpoint of the protection of private data and also from a business perspective, complete data transparency within a DLT system is not desirable. It is therefore out of the question for financial companies that all trading activities of a system participant might be traced by third parties, as is the case for Bitcoin. While there are encryption technologies that address these concerns, implementation must weigh the various requirements against each other, such as the degree of anonymity of the data vis-à-vis third parties vs. data transparency vis-à-vis the competent supervisory authority or regulator.

Loss/theft: While encryption technology and digital signatures increase data security in principle, effective protection against loss or theft also depends to a large extent on the administration of private keys. For example, several of the major thefts of tokens were due to the improper administration of private keys. Great importance must therefore be attached to the safekeeping of private keys.

30 At most two of the three properties of *consistency, availability,* and *partition tolerance* can be guaranteed at the same time.

Governance

A decentralised system faces the challenge of establishing clear and unambiguous rules and enforcing them where necessary. While the rules for a completely decentralised DLT system such as Bitcoin exist exclusively at the protocol level, other systems (such as Ethereum) often have (minimal) institutional rules beyond the protocol. This has the advantage that the protocol itself can be adjusted according to a specified procedure (which is a fundamental challenge of the Bitcoin network). At the same time, such solutions move away from the principle of the "pure" blockchain and come closer to existing electronic systems and infrastructures. Effective governance mechanisms are important to ensure that DLT systems (and their protocols) can also be continuously adjusted to new technological developments (see above, for example, on developments in the field of encryption technologies).

3 Applications of DLT in the financial sector

3.1 Introduction

From a functional point of view, a blockchain serves two purposes:[31] firstly, it clarifies what share in what object can be attributed to whom at what point in time, as well as who transferred that share to whom, to what extent, and at what point in time. Moreover, the growth of a blockchain also ensures the irrevocability and immutability of the registered transactions over time. Secondly, blockchain technology provides transparency with regard to the registered transactions, which can strengthen participants' trust in the system. Part of the potential of decentralised, peer-to-peer systems is that they might replace centralised systems (in whole or in part) and in that way bring about the structural change of industries through disintermediation. This is also true of the financial sector.

In principle, it is conceivable that a DLT system could allow the authentication or settlement of transactions by a central financial intermediary (e.g. bank, insurer) and potentially increase efficiency. The main difference between DLT and traditional technologies for financial market transactions is that DLT conceptually makes a direct electronic transfer of value possible between the participants in the network without having to involve an entity that manages the accounts. Since the principle of distributed consensus can increase security and stability in the system, decentralised systems could also be suitable for handling particularly important data (e.g. securities trading, payment transactions, and asset management).

Several examples of DLT applications in the financial sector are discussed below.

3.2 Corporate and project financing through initial coin offerings (ICOs)

3.2.1 Preliminary remarks

While larger companies often obtain financing through traditional financial intermediaries such as banks or the capital market, important sources of funding for smaller companies and start-ups include venture capital firms, promotion programmes and, increasingly, crowdfunding platforms.

ICOs are a new DLT-based mechanism with which companies, private individuals, and communities of interest can raise funds for their business or project. In contrast to traditional sources of financing, however, an ICO does not require a financial intermediary, but rather can be designed as a pure *peer-to-peer* mechanism. This means that projects and investors can connect directly with each other and carry out transactions on a global basis.

3.2.2 Market size worldwide and in Switzerland

There are currently no official statistics on the number of ICOs launched and the funding volume achieved. Nevertheless, figures from various private sources point to strong growth in the ICO market. According to Coindesk,[32] around 650 ICOs worldwide have been carried out so far in 2018, raising funds in the amount of roughly USD 17 billion (see figure 4).

31 Drescher 2017: 206.
32 See www.coindesk.com (as at 6 December 2018).

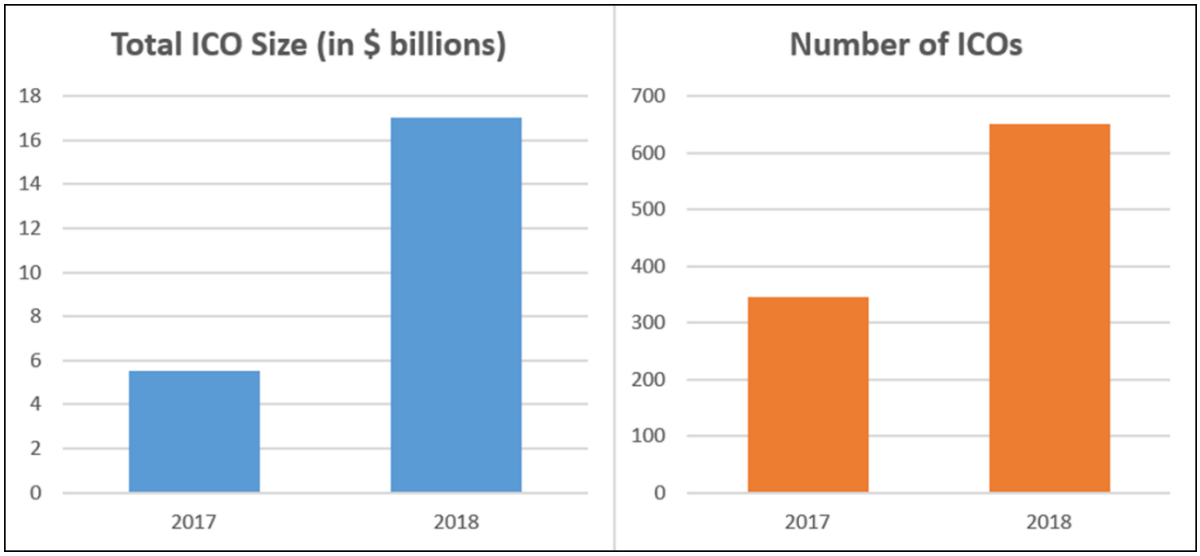

Figure 4: ICO size and number worldwide (Source: Coindesk 2018)

3.2.3 How ICOs work

To convince project investors, the token issuer publishes a "white paper".[33] White papers for ICOs may be structured in very different ways. As a rule, this is a document made available to the public by the token issuer that describes and advertises the ICO, contains a sort of business plan for this purpose, and presents the structure of the ICO as well as the technical and legal steps involved in the ICO. The white paper usually includes descriptions of the project, the team, the development roadmap, conditions of the token issue, as well as technical and functional properties of the token.

In most cases,[34] a pre-sale takes place before the actual ICO. In contrast to the ICO, this pre-sale is aimed at selected investors who are usually able to invest larger sums of money in the token at preferential conditions.

Depending on the design of the ICO, tokens may be put into circulation already at the time the funds are raised. This is done on an already existing blockchain. In the case of other ICOs, the only prospect raised at the time of the ICO is that investors will receive tokens in the future and that the tokens or the underlying blockchain still have to be developed (pre-financing). Another possibility is an advance sale. Here, investors receive tokens with the option of obtaining or exchanging them into other tokens.[35]

ICOs themselves can be structured very differently, but there are a few fundamental elements that are described below using the example of an ICO based on the Ethereum blockchain. The Ethereum blockchain is currently especially suited to carrying out ICOs. This is in part due to the functionality of smart contracts and the ERC20 standard. ERC20 is a standardised set of rules for the design of tokens, *inter alia* defining the transferability between different addresses and access to information stored in the token.

---

33 Recently, there has been a trend toward shorter publications called "light papers".

34 According to Zetsche/Ross/Douglas/Föhr 2017, more than 60% of all ICOs are not really "initial" public offerings.

35 See also FINMA 2018a: 3.

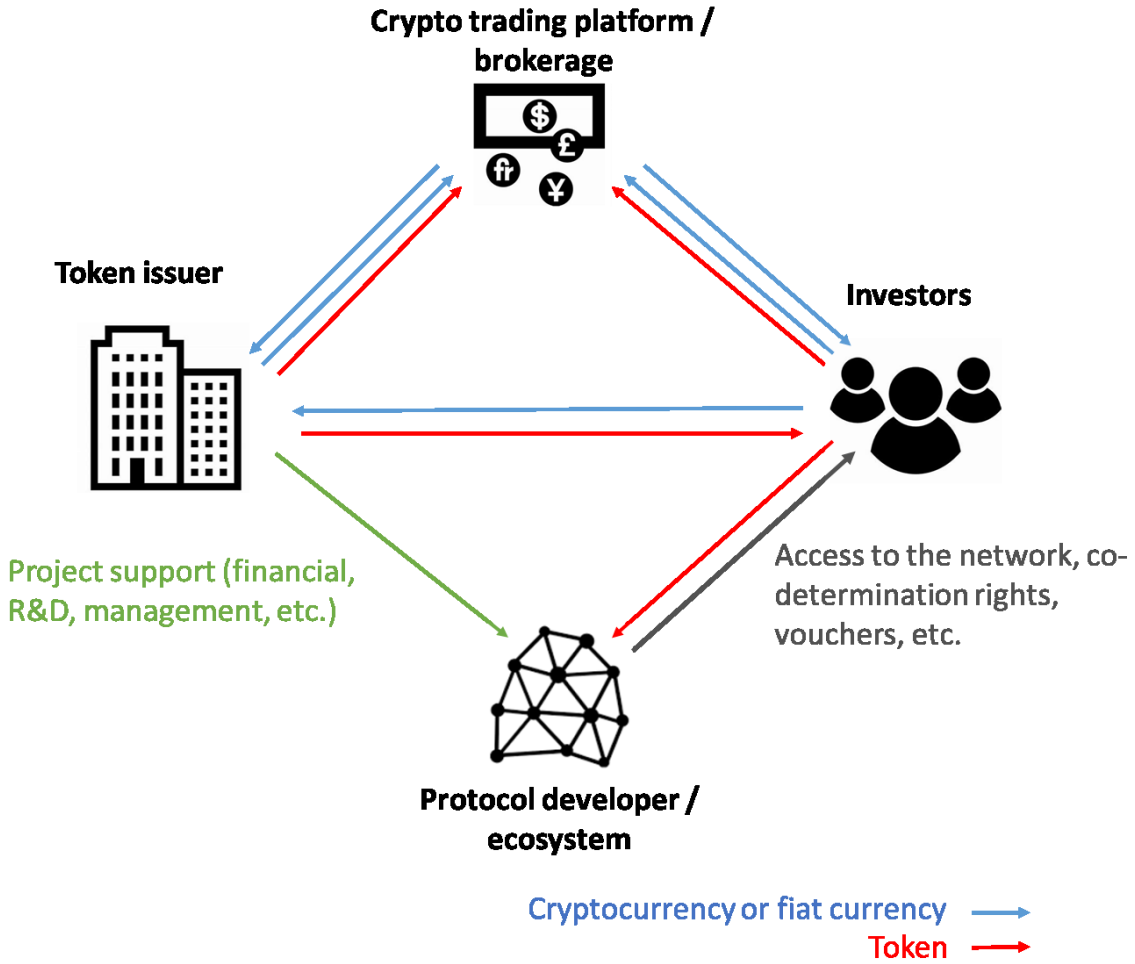

Figure 5: Typical ICO design (own illustration)

In an ICO, investors transfer funds (usually in the form of cryptocurrencies such as Bitcoin or Ether) to the token issuer (see figure 5). The use of these funds is described in more or less detail in the white paper and constitutes fundamental information for the investment decision of individual investors. In the example of ERC20, investors transfer a certain amount of Ether from their Ethereum wallet to the smart contract address of the token issuer. Typically, this smart contract collects Ether from various investors until, for example, a pre-defined time period (e.g. three months) has been exceeded or a maximum amount of tokens (cap) is reached. If certain criteria are not met (e.g. the cap is not reached), the smart contract automatically sends the collected Ether back to the various wallets. If all predefined criteria are met, the Ether is forwarded to a wallet of the token issuer and is made available to it. At the same time, the smart contract sends new, project-specific tokens created according to the ERC20 specification to the wallets of the investors.

The token issuers use the funds for their projects. This is typically done by using the raised funds for research and development, marketing activities, development of the protocol, etc.

Investors can use their wallet to access the tokens allocated to them that have been newly created in the ICO. They basically have three options: they can (1) leave the tokens in their wallet and speculate on a gain in value, (2) exchange the tokens for other tokens or conventional currencies on a crypto trading venue, or (3) get involved in the ecosystem of the newly created project. Investors may make use of the specific characteristics of the token for that purpose (see next section), or the tokens may be stored in a proof-of-stake system for validating transactions.

3.2.4 Characteristics of tokens

The design of tokens can be highly customised and vary considerably. This section enumerates the basic technical distinctions and examples of functional characteristics. The legal classification is discussed in sections 5.1 and 6.2.

From a technical perspective, a fundamental distinction can be made between native and non-native tokens. A native token is implemented in the protocol of a blockchain and is key to its functioning. Typically, the validation of blocks within a blockchain is compensated with this native token. The token is thus an important component of the consensus mechanism. Examples of native tokens are Bitcoin and Ether.

Non-native tokens, on the other hand, are implemented not in the protocol of a blockchain itself, but rather in a second-layer protocol based on it or in an application. Such tokens are logged on the underlying blockchain and allocated to the participants in question, but they are not an integral part of this blockchain itself. In other words, the blockchain also works without these tokens. An example of non-native tokens are all the tokens that meet the ERC20 standard. While these tokens are all mapped on the Ethereum blockchain, the Ethereum blockchain works with its own native token (Ether).

Depending on its individual design, a token can fulfil various functions and offer different benefits to the investor. This benefit may arise directly from the service associated with the token. An example of this is Bitcoin. A Bitcoin owner can use it as a means of payment or as an investment without having to contribute to the Bitcoin system (e.g. as a miner). However, a token may also offer the possibility of participating actively in a system. Whoever owns tokens may contribute, for example by participating in votes, providing information, supplying editorial contributions for forums, etc. The incentive to contribute may consist in a direct payment in the form of tokens or in added value from the use of the network (e.g. Information).

3.2.5 Potential of ICOs

Financing through an ICO has significant structural differences compared with classical financing models and offers various advantages and disadvantages.

The particular advantages include the wide (global) reach through a purely digital distribution of the tokens; the quick realisation of ICO-based financing compared with many other financing options; possibly the liquidity of the investment (if tokens are traded on a trading venue); and the inclusion also of (very) small investors. Additionally, investors may at the same time become users of the project financed by the ICO (thus achieving better customer loyalty), and an opportunity is created to finance networks.

Disadvantages include the large number of investors, legal uncertainties, and the number of dubious projects. Furthermore, the high volatility of the token prices can have a negative impact on the project itself, and investors often use the tokens solely out of speculative interest (without contributing to the ecosystem).

3.3 Payment transactions

3.3.1 Preliminary remarks

Payments are a central element of economic activity. Virtually all transactions, whether purchase of goods or compensation for services, are associated with a payment.

The basis for every payment is the means of payment (or the payment instrument).[36] This includes physical cash, i.e. coins and banknotes. The relevant characteristics of cash are that it makes transactions possible without intermediaries (i.e. peer-to-peer) and step by step.

[36] See SNB 2018.

Moreover, in the case of cash, the authenticity of the means of payment itself is verified, not the legitimacy of the owner to dispose of it. Coins issued by the federal government and banknotes issued by the Swiss National Bank are furthermore considered legal tender.

But payments may also be made cashless, i.e. electronically. Widespread electronic means of payment (or payment instruments) include payment cards (debit and credit cards), credit transfers, direct debits, and electronic money (e-money). In account-based cashless payment transactions, payments are debited from a payer's account and credited to a payee's account.[37] Account-based cashless payments require one or more intermediaries to keep records of the credit balances and adjust them accordingly once a payment transaction has been made. Account management by a third party is necessary to prevent double-spending in account-based cashless payment transactions. In contrast to cash, it is not the authenticity of the electronic means of payment that is verified in account-based cashless payment transactions, but rather the payer's right to dispose of the credit balance.

3.3.2 DLT in payment transactions

Making electronic payments possible without having to resort to a centralised third party is one of the first and most prominent applications of DLT. For example, electronic payment transactions are explicitly cited in the Bitcoin article.[38] Bitcoin and DLT have solved the double-spending problem, i.e. the problem that electronic credit balances might be used more than once if there is no centralised account management. The historisation of past transactions in hash chains and digital signing of the transaction execution make it possible to exchange digital values without trustworthy third parties.

There are meanwhile many tokens with payment functions. The characteristics of these tokens differ significantly depending on the type of issue (decentralised or centralised), the token issuer (bank or non-bank), and the existence of any underlying assets of the token (e.g. securities, commodities, etc.).

3.3.3 Potential of DLT

Payment transactions, especially in retail, are a mass business. This means that the demands on throughput (number of transactions a payment system can process per second) are very high. Major card systems (e.g. Visa, Mastercard, American Express, etc.) process several thousand transactions per second. As explained above, the SIC system also processes approximately 2 million transactions per day (with peaks of up to 7.5 million transactions per day). The limitations on scalability and throughput described in section 2.3 thus constitute a fundamental problem for the use of tokens in payment transactions.

A distinction should be made here between domestic and cross-border payment transactions, however.

3.3.3.1 Domestic payment transactions

Domestic cashless payment transactions generally function smoothly in industrialised countries, which means that they are fast and inexpensive. In addition, efforts are underway in many countries to enable cashless payments in real time, around the clock, and at low cost.[39] Given these efforts and the limitations mentioned above, the potential of cryptocurrencies to enhance the efficiency of domestic payment transactions in industrialised countries appears

---

37 Depending on the cashless payment instrument, this transfer may be performed in very different ways: a credit transfer, for example, is initiated by a payment instruction from the payer to transfer funds to the payee. A direct debit is a debit of the payer's payment account initiated by the payee with the payer's consent.

38 Nakamoto 2008: 1.

39 See CPMI 2016.

to be rather limited. In countries with a less developed payment infrastructure, cryptocurrencies may indeed have some potential for use as an alternative means of payment.[40]

3.3.3.2 Cross-border payment transactions

Compared to domestic payment transactions, cross-border payments are slow, costly, and less transparent, and opportunity costs are accordingly high.[41] This means there is significantly greater scope for efficiency gains in cross-border payment transactions. In addition, there is greater complexity (large number of different currencies, actors, and processes). As explained above, DLT could offer advantages especially in such complex areas, given that, for instance, bilateral reconciliation between the actors is no longer necessary thanks to the shared reference database. However, also in cross-border payment transactions the question arises as to whether DLT offers decisive advantages compared with improvements that may be made on the basis of centralised technologies. Moreover, fundamental questions arise when changing over to a new technology, e.g. concerning interoperability with existing systems.

3.4 Securities trading, clearing, and settlement

3.4.1 DLT in securities trading, clearing, and settlement

In principle, three phases can be distinguished in the life cycle of securities (after their issue):[42] trading, clearing, and settlement. These processes are transacted via financial market infrastructures.[43]

One of the key characteristics of DLT is making verified information available to many parties at the same time. It is therefore especially attractive for complex processes in which many actors have to coordinate with each other.

This is the case in the securities sector: it is a system involving many different actors who trade, settle, and manage securities. These market participants, i.e. securities dealers, banks, financial market infrastructures (such as settlement systems and central securities depositories), have to reconcile a lot of information bilaterally for each transaction. For instance, banks must monitor their securities holdings at depositaries and reconcile them with their internal accounting. This coordination effort leads to high operational costs. DLT-based applications could reduce the coordination effort by assuring synchronously that all involved parties have the same level of information.

3.4.2 Potential of DLT

Possible advantages of DLT in the area of securities include in particular a higher degree of transparency, efficiency, resilience, and automation in the settlement of securities transactions.[44]

- **Transparency**: The very complex coordination mentioned above between the participants could be reduced substantially thanks to the distributed and synchronised information.
- **Efficiency**: An entry in the shared database could be considered simultaneously as conclusion of the trade, clearing, and settlement. Efficiency gains through DLT are not to be expected primarily from the actual settlement, however, but rather from downstream processes in the management of securities (e.g. corporate actions).

---

40 See IMF 2018a.
41 See CPMI 2018a.
42 See section 3.2.
43 See section 6.4.
44 See Deutsche Bundesbank 2017.

- **Resilience**: As discussed in section 2.5, distribution of the data in principle increases the resilience of the network, since the risk of the single point of failure is reduced by the distributed validation. At the same time, the increase in the number of validating nodes also creates new gateways for possible attacks. These two aspects must therefore be carefully weighed against each other.
- **Automation**: Automated or self-executing contracts (smart contracts, see section 2.3) promise increased efficiency for transactions that require reconfirmations or guarantees from business partners. In the case of collateral management or trust accounts, smart contracts could trigger and enforce actions themselves without third parties having to initiate (or prevent) them. The automatic triggering of payments (interest, dividends) and the depositing of further self-triggering actions (especially in the case of low trading/exotic securities) has the potential to increase efficiency. Smart contracts can also ensure the settlement of multiple transaction steps in complex transactions. If, for instance, a component of such a transaction is not executed (for example because one party does not have sufficient credit or a system is not available), the smart contract could ensure that all steps already taken are reversed. This ultimately increases security and reliability for all parties.

Due to the possible advantages of DLT in the securities sector, it is conceivable that such a project could also be implemented as part of the central financial market infrastructure. In July 2018, for example, the Swiss exchange operated by SIX announced its intention to establish the world's first fully integrated infrastructure for the trading, settlement and custody of digital assets. It is still too early to see the effective benefits of a DLT-based solution compared with current approaches. If, however, DLT-based systems should prevail in the securities sector, the question also arises as to the extent to which the cash side of these transactions might be processed in such a system.[45]

3.4.3 Payment tokens for settling securities transactions

3.4.3.1 Instability of value and credit risk of payment tokens

The lack of or insufficiency of value stability of tokens poses a fundamental problem for cryptocurrencies without a link to a conventional currency (such as the Swiss franc). For this reason, it is probable that tokens will be linked in future to a currency issued by a central bank, at least indirectly. Such a link can for example be achieved by a 1:1 conversion: payment tokens are exchanged 1:1 against conventional currency. This achieves value stability while taking advantage of the possible technological advantages of DLT-based systems.

In the case of time-critical payments involving high amounts, credit and liquidity risks are also taken into account in addition to the demands on stability of value.[46] Accordingly, international standards[47] and the National Bank Ordinance[48] require that, wherever possible and practicable, systemically important financial market infrastructures settle payments by transferring sight deposits at a central bank (i.e. central bank money). Otherwise, such a financial market infrastructure is required to use a means of payment that has little or no credit and liquidity risk.

---

45 See section 3.4.3.

46 Credit risk arises, for instance, if a settlement bank becomes insolvent. If a financial market infrastructure settles on its own books, the participants are exposed to the default risk of the settlement institution itself.

47 CPMI/IOSCO 2012: Principle 9.

48 Art. 25 NBO.

3.4.3.2 Possible design of a payment token for settling securities transactions

The question arises in this context as to the possible design of a payment token for settling securities transactions.[49] The issuing institution of such a payment token and the design of the token as such must be taken into account in this regard.

In principle, the cash side could be integrated directly into the DLT-based infrastructure. To achieve this, the (private) operators of this infrastructure could issue a payment token on the DLT system. The tokens mapping the securities would then be settled step by step against these payment tokens. Various consortia are currently working on such solutions.[50] This is an example of how a market solution could be used to make the cash-side settlement of securities on the distributed ledger possible. Apart from technological questions, the focus is especially on legal and regulatory issues, in order to ensure the security and efficiency of such a solution. In this context, tokenisation of central bank money for the settlement of transactions between banks would also be conceivable.[51]

3.5 Asset management

DLT also has potential use cases in the field of asset management. DLT applications can be used for individual aspects of asset management or as a basis for its entire business model. Examples of such use cases relevant to asset management include:

- **Publication of information**: Like other financial intermediaries, asset managers must also publish information (e.g. regulatory reporting, traded prices, etc.). DLT could enable or at least simplify the storage of data as well as the paperless transmission thereof appropriate to the addressee.
- **More efficient processes**: Smart contracts might be used to automate the onboarding of clients, document management, dividend transfer, etc.
- **Tokenisation of fund units**: If fund units were structured in the form of tokens, payments into and out of the fund could be simplified and made directly via DLT. This would make it easier for funds to appeal directly to retail clients and thus make them less dependent on intermediaries. Tokens would also be tradable on the secondary market.
- **Complete DLT-based asset management**: A combination of the examples mentioned above could be used to represent a complete DLT-based asset management business model. However, this would necessitate that only DLT-based assets would be invested. Should the tokenisation of assets continue to increase, a wide range of investment opportunities might arise in the future.

3.6 Trade finance

DLT applications are also being developed in the area of trade finance. In the near future, they could be particularly relevant from a Swiss perspective because of their increasing importance for the Swiss commodities sector.

---

49 One possibility for settling securities tokens without a payment token would be a technical interface between a DLT system and an existing payment system. Payment instructions would be exchanged via this interface, similar to the current solution between the securities settlement system SECOM and the payment system Swiss Interbank Clearing SIC. For a direct settlement of securities against payment, however, some adjustments would have to be made, e.g. the operating hours of the two systems. It is also questionable whether the advantages of DLT would come fully into play with such a solution: potential advantages of DLT also arise with downstream processes.

50 E.g. the Utility Settlement Coin (USC) consortium or the R3 consortium.

51 See also CPMI 2018b.

Companies and consortia in Switzerland are currently developing projects for the use of DLT in this field, such as trade finance platforms, applications for real-time process monitoring, and projects for secure exchange among all participants.

The functioning of DLT applications is fundamentally comparable to that of other applications. The platforms can also be thought of as distributed databases. Each transaction or transaction step is part of a block that is integrated into the chain as it is executed. The use of paper in cross-border business transactions is still widespread. It is not uncommon for the waybill to take more time than the actual transport and delivery of the goods.

There is potential in the following areas in particular:

- ***Efficiency***: Standardisation and digitisation of the necessary documents could reduce costs and margins of error significantly. The significantly shorter duration of the transactions would also be beneficial for all participants in terms of liquidity requirements. Individual transaction steps can be automated using smart contracts. This leads to further time savings.
- ***Security***: The security of transactions can be improved, and the authenticity of documents can be ensured. Once a block has been included in the chain, it can no longer be changed. The system prevents any subsequent changes to the transaction history. Fraud and counterfeiting – which occur frequently in this context – could be prevented.
- ***Decentralisation of information***: The use of DLT for data in trade finance could increase confidence among intermediaries and clarify who owns the information. Existing central trading platforms, if developed by individual companies or consortia, may raise governance issues (who owns the platforms and the data).
- ***Transparency and traceability***: Real-time coordination of transaction steps among all participants (exporter, importer, dealer, financing bank, insurer, associated services) is a further advantage in terms of transparency and traceability.

DLT applications could also be extended to include the management of complex value chains, for instance by linking the management of financial flows with that of flows of goods. In this way, distribution could be transferred to the blockchain, linking physical elements and data (seals, sensors, microchips, GPS data) and the potential use of tokens with the trading platform.

For Switzerland, the changes bring opportunities and challenges. Innovative Swiss projects could create a digital Swiss ecosystem for commodity trading. Switzerland could use synergies between the industry and innovative Swiss technologies as a competitive advantage. Such applications would have to be designed for use by the whole industry (and not just individual companies) at the national and international level. This would not only strengthen application of the technologies as such, but also Switzerland as a location.

On the other hand, DLT applications might also destabilise established structures in the sector. More direct contact between parties to transactions could make more attractive bilateral forms of financing possible for non-banks, which could also be a disruptive element for banks currently active in trade finance. More transparency in the transaction chain and accordingly also of prices, given already very low margins, could represent a challenge for traders. Finally, the non-negligible costs required for the development of DLT applications must also be taken into account. For Switzerland, it is therefore important to create a favourable framework for the development of a digital ecosystem that strengthens the competitiveness and interconnectedness of the Swiss business location vis-à-vis other countries.

3.7 Insurers

The business of insurers consists essentially in obtaining as reliable information as possible about their current and future clients in order to use this information to calculate an insurance premium that is sufficient from an actuarial point of view and then to pay out the compensation to which the insured party is entitled in the event of a claim. DLT can be relevant at various points in this process:

Public blockchains as feeders for big data: When obtaining client information, it is crucial that the data is available on a large scale and in digital form in order to categorise clients. Permissionless blockchains can play a role insofar as they can be used by insurers as (additional) sources of information. The technical immutability of the data can be particularly advantageous here, given that it prevents subsequent data manipulation. But this does not guarantee the accuracy of the data: false information is still false, even if it is stored on a blockchain.

Use of smart contracts: When an insured event occurs, the insurer generally incurs high claims processing expenses. The insurer has an interest in avoiding lengthy claims assessments and legal disputes. Smart contracts could be part of a solution in this regard. If, for instance, a blockchain were to reflect the current status of motor vehicles, a smart contract could automatically perform the insurer's accident payment to the injured party. A condition would be that the necessary information would also be available digitally and mapped in the blockchain; this means, for example, that the police would have to enter every accident and automobile repair shops would have to enter every repair on the blockchain.

Also in the case of parametric insurance, smart contracts could play a role in the future: in this type of insurance, the insurer does not pay an amount equal to the loss incurred in the event of a claim, but rather an amount independent of the claim. This amount is calculated according to external parameters, e.g. the strength of an earthquake or storm. A homeowner thus receives a payout if an earthquake or storm occurs, but whether and to what extent the home itself has actually been damaged is irrelevant. Parametric insurance relies on the existence of objective – usually physical – parameter measurements. These are supplied by external institutions; in the example mentioned above, an earthquake or weather station. The concept of parametric insurance implies that the contracting parties have confidence in the quality of these institutions. The internet of things (IoT) could likewise increase the application possibilities of parametric insurance in the future, for example if smart contracts of insurance policies are linked to sensors in all conceivable areas of life (such as water sensors in the basement for flood insurance; position sensors on bicycles for theft insurance; acceleration sensors in cars for comprehensive car insurance, etc.).

Blockchain Insurance Industry Initiative: Several insurers, including from Switzerland, have formed a consortium (B3i) to examine how a distributed ledger controlled by insurers could be used to administer reinsurance contracts.

3.8 Regulatory disclosure and reporting

Depending on the architecture of the blockchain used, authorisation to make entries in the database, validate them, and/or access them can be assigned as required. In such cases, the potential areas of application include accounting as well as regulatory and contractual reporting obligations, where account postings, financial transactions, documents, and other facts are mapped on a blockchain and thus stored in a non-falsifiable way. Access rights for selected third parties, such as external auditors, supervisory authorities, and regulators or a contracting party would permit them to retrieve the data virtually in real time and to process them further for their respective purposes.

4 International environment

4.1 Developments at the international level

Worldwide, there is considerable variety in the legislation governing blockchain-based activities and their treatment by the competent authorities.[52] A smaller number of jurisdictions, for instance, prohibits certain services in connection with tokens (e.g. trade) and/or ICOs. In contrast, a growing group of jurisdictions is developing tools to actively promote the development of crypto assets and at the same time to limit risks. Numerous jurisdictions are currently in the process of developing specific legislative measures to regulate blockchain systems, ICOs, and other activities relating to crypto assets. The approaches chosen are very diverse and also differ with respect to their chosen focus (e.g. civil law vs. financial market law).

4.2 Multilateral developments

Due to the potentially far-reaching consequences, the interest of international bodies in the financial area in blockchain technology is currently high. The group of the 20 most important industrialised and emerging countries (G20) is assuming a coordinating function by delegating mandates to other bodies. The still new topic of blockchain is attractive for many international bodies, and the distribution of labour among them has not yet been conclusively clarified.

The OECD is addressing the blockchain issue on a relatively broad front. Since 2014, the OECD has published a number of research and policy papers, including on the impact of the technology on tax policy and investor protection. On behalf of the G20, it is currently analysing the risks arising from blockchain technology for tax transparency. In regard to investor protection, the OECD is looking at the application of the G20/OECD High-Level Principles on Financial Consumer Protection to markets for tokens and the need for new regulations to ensure the desired investor protection in token markets, while still allowing the development of useful innovations.

In recent years, the International Monetary Fund (IMF) has published various working papers and reports on opportunities and risks arising from blockchain technology applications. In the view of the IMF, ongoing rapid growth of crypto assets could lead to new vulnerabilities in the international financial system.[53] The IMF has identified further risks, including in the fight against money laundering and terrorist financing. At the same time, the IMF has also identified numerous opportunities of the technology. These include the potential to make the payment system more efficient and, especially in developing countries, to strengthen property rights and market confidence and to facilitate private investment. The IMF is aiming for an internationally coordinated approach to the topic.

Within its scope of responsibilities, the Financial Action Task Force (FATF) is examining issues relating to virtual assets. In this context, it decided in its plenary in October 2018 that virtual asset service providers (VASPs) are expressly covered by the FATF Recommendations and that measures to combat money laundering and terrorist financing must be applied. The FATF is currently working on clarifying exactly how these requirements are to be applied to VASPs. In addition, the FATF will revise its 2015 guidance for a risk-based approach to VASP regulation and develop guidance for operational and law enforcement authorities to combat money laundering and terrorist financing in relation to VASPs.

---

52 See e.g. PwC Global ICO Compass. Available at: https://www.pwc.ch/en/industry-sectors/financial-services/fs-regulations/ico.html (as at 18 October 2018); Report of the US Law Library of Congress of June 2018 on Regulation of Cryptocurrency in Selected Jurisdictions. Available at: https://www.loc.gov/law/help/cryptocurrency/regulation-of-cryptocurrency.pdf (as at 18 October 2018).

53 See IMF 2018b: 22.

One of the most active bodies with regard to blockchain is currently the Financial Stability Board (FSB). Between 2017 and 2018, the FSB examined how blockchain technology, and in particular the formation of bubbles in the crypto asset market, might impact the stability of international financial systems. According to the FSB, the markets for crypto assets do not constitute a threat to financial stability in light of their low volume for now.[54] The G20 has adopted this position for the time being. The FSB accordingly does not currently intend to become actively engaged in regulation governing crypto assets or specifically tokens. Markets for tokens are developing rapidly, however. In cooperation with the Committee on Payments and Market Infrastructures (CPMI), the FSB has developed a methodology for monitoring the stability risks arising from crypto assets. The FSB is observing the further development of these markets as part of its general monitoring of stability risks.

Since 2015, the Committee on Payments and Market Infrastructures (CPMI) has been carrying out various analyses of blockchain technology as part of its thematic working groups, and it offers the participating central banks a forum on the topic. The focus is on ensuring the security and efficiency of financial market infrastructures in a changing technological environment. Since 2015, the CPMI has published several reports on blockchain and the role of central banks in payment transactions.[55] Ongoing analyses examine the possibilities of payment tokens issued by central banks or covered by central bank money for the settlement of transactions between financial institutions.

The Basel Committee on Banking Supervision (BCBS) examines blockchain from the risk perspective for banks. The BCBS is currently examining the possibility of carrying out a data collection to quantify the exposure of banks to tokens. In addition, the BCBS will take stock of the national practices of its members to clarify any need for regulatory adjustments to the treatment of tokens in the various risk categories (credit risk, counterparty risk, market risk, liquidity risk, etc).

The International Organization of Securities Commissions (IOSCO) follows developments in blockchain technology primarily from the perspective of customer protection. The IOSCO has already issued several investor warnings on the development of the token markets. The IOSCO has also established a Consultation Network to promote exchanges among national supervisors, in particular with regard to cross-border implications of customer protection in token markets. There are no foreseeable regulatory activities on blockchain technology at the IOSCO, however.

In addition, the UN Commission on International Trade Law (UNCITRAL) is monitoring blockchain as part of its general work on the digital economy. Its current focus is on problem analysis, however.[56] Finally, the International Organization for Standardization (ISO) is working on the standardisation of blockchain technology (uniform definitions, etc.).[57]

4.3 Switzerland's positioning in multilateral bodies in the financial area

In multilateral bodies in the financial area, Switzerland works to ensure that the innovative potential of blockchain technology is maintained and that the associated risks, particularly in the fight against money laundering and terrorist financing, are addressed in a coordinated manner. At the international level, Switzerland emphasises the benefits of a balanced,

54 See e.g. FSB 2018.
55 See CPMI 2015; CPMI 2017; CPMI 2018b. See also CPMI 2016; CPMI 2018a.
56 See Report of the United Nations Commission on International Trade Law, 51st Session from 25 June to 13 July 2018: para. 248 and 253(b). Available at www.uncitral.org > Working Documents > Commission > Report of the United Nations on International Trade Law of its Fifty-first Session.
57 See e.g. ISO Technical Committee ISO/TC 307; additional information available at: www.iso.org > Taking part > Who develops standards > Technical Committees > ISO/TC 307 (as at 18 October 2018).

principle-based, technology-neutral, and activity-based regulatory approach to blockchain and DLT-based financial services.

In the Federal Council's view, there are a number of specific areas relating to blockchain/DLT in the current phase where multilateral coordination can offer added value. This concerns, for example, the development of a common international language in the field of crypto assets and, in general, an exchange and deepening of the understanding of crypto assets. A better understanding of technological and economic developments as well as possible regulatory shortcomings is essential before internationally coordinated work on the regulation of blockchain or DLT technologies can be advanced.

From a Swiss perspective, however, it is already clear that international cooperation especially is indispensable and urgent with a view to reducing money laundering and terrorist financing risks in connection with crypto assets. Within the FATF, Switzerland actively advocates a coordinated international approach and clarification of open questions. Switzerland also supports international work on monitoring possible financial stability risks in the context of crypto assets.

5 Legal basis under civil law

5.1 Legal classification and transfer of tokens

5.1.1 Data ownership rights

There are currently many discussions in very different contexts regarding who owns data and who can determine the use and economic exploitation of data. These questions also play a central role in the legal classification of tokens and the assessment of how they can be transferred legally. The introduction of data ownership is one of the possible solutions being discussed.

5.1.1.1 The situation under current law

Current law does not provide for a general right of ownership of data. However, various legal instruments already today convey ownership-like legal status under certain conditions and due to their fundamental neutrality with respect to technology.[58]

For personal data, the Federal Act on Data Protection (FADP) and, on a subsidiary basis, the law of personality provide for individual rights that come close to the right of ownership.[59] But even for data not relating to persons, legal rights similar to ownership already exist today. Under certain conditions, competition law provides a certain degree of protection alongside copyright law and other intellectual property rights. If there is damage and causality and if unlawful conduct and fault are shown, there are also rules under tort law which grant protected, ownership-like legal status for digital data. Finally, contracts can also be used to assign ownership-like status to digital data.

Some of the relevant academic literature argues that the rules of chattel ownership under Articles 713 et seq. of the Swiss Civil Code (CC)[60] apply to data and that the resulting rights are applicable and offer corresponding protection.[61] According to prevailing opinion, however, the rules of property ownership are not applicable to digital data, especially due to their lack of physicality.[62] The concept of property under Swiss law covers only three-dimensional, physically tangible objects.[63] While under Article 713 CC, chattel ownership also relates to forces of nature that may be the subject of legal rights, the rules of property law apply to them only analogously.[64] The proposal to apply the rules on intellectual property analogously to digital data[65] has likewise not become the majority opinion.

5.1.1.2 The question of introducing the concept of data ownership

Whether the time is right to create the concept of general data ownership is currently the subject of intense academic debate.[66] It appears, however, that the opinion is prevailing that there is no need for the creation of general data ownership. According to this opinion, there is agreement in principle that the applicable law, under certain conditions, conveys sufficient ownership-like legal status that is applicable either specifically or by virtue of its neutrality with regard to technology. In addition, a majority of scholars argue that the introduction of data ownership would create new problems rather than provide a solution to any outstanding

58 See Thouvenin/Weber 2017: margin no. 8; Weber/Thouvenin 2018: 49 et seq.
59 Benhamou/Tran 2016: 572-573; Thouvenin 2017: 22-23; Weber/Thouvenin 2018: 46.
60 SR **210**
61 Eckert 2016: 245 et seq.
62 See e.g. Fröhlich-Bleuler 2017: margin no. 13 et seq.; Hürlimann/Zech 2016: margin no. 8; Weber 2015: 30; Weber/Thouvenin 2018: 49; on tokens as property, see also section 5.1.1.3 and the references in footnote 80.
63 Rey 2007: margin no. 66 et seq., 81; Schmid/Hürlimann-Kaup 2017: margin no. 7.
64 Rey 2007: margin no. 86 et seq.
65 Benhamou/Tran 2016: 572 et seq.
66 Thouvenin/Früh/Lombard 2017: 34.

issues.[67] Also according to the federal government's data policy, the existing legal bases with regard to data ownership are not to be fundamentally revised at this time.[68]

At the same time, however, it must be noted that advancing digitalisation creates specific legal problems which the Swiss legal system does not cover. Open questions exist, for example, regarding the treatment of data under inheritance and bankruptcy law[69] and the treatment of cryptocurrencies. To solve these and other new specific problems that arise, there is selective need for regulation. First steps in this direction can already be seen. For example, the draft of the totally revised Federal Act on Data Protection provides possible solutions for the treatment of personal data under inheritance law.[70] In this context, the Federal Council is also examining whether the right to data portability under the European General Data Protection Regulation,[71] which conveys a right of data subjects to receive the personal data concerning them, should be adopted. Finally, policymakers are calling for the introduction of a right to restitution of data in the event of bankruptcy of cloud providers.[72] The treatment of data under bankruptcy law[73] and the legal classification of tokens[74] are among the topics covered by this report.

5.1.1.3 Ownership rights to tokens?

As shown, the prevailing doctrine holds that no rights in rem can exist *de lege lata* with respect to data.[75] But a minority opinion now seeks to classify tokens – as distinguished from data – as property:[76] it is argued that sovereignty over tokens can be exercised exclusively by controlling the private key, and that the decentralised public register creates publicity as well.

It should first of all be noted that full publicity – as in the case of objects – can be achieved only through public registers, which is not the case for all blockchains.[77] But above all, the element of physicality continues to be central for existing property law.[78] This element cannot be fulfilled by tokens, given that they are not physical. Tokens can therefore never actually be handed over, in the true sense of the phrase. Even proponents of the classification of tokens as property resort to the forced execution of the right to a token by way of physical surrender of the password, the private key.[79] Tokens cannot be treated like moveable objects. The prevailing doctrine in fact almost unanimously rejects the classification of tokens as chattels.[80] Because tokens are not physical objects, they thus cannot be subject to an ownership right.

---

67 E.g. Weber/Thouvenin 2018: 60 et seq.

68 See the press release by the Federal Council of 9 May 2018 on measures for a future-oriented data policy in Switzerland ("benchmarks"). Available at www.admin.ch > Documentation > Media releases (as at 18 October 2018).

69 BGE **128** III 388; BGE **105** III 14; BGE **90** III 92. See e.g. Hauser-Spühler/Meisser 2018: 1, 10; Neuenschwander/Oeschger 2017: margin no. 11; Weber/Thouvenin 2018: 58.

70 Art. 16 D-FADP (Draft of the Federal Act on Total Revision of the Federal Act on Data Protection and amendment of other enactments on data protection, BBl **2017** 7193, 7213).

71 Art. 20 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).

72 Parliamentary initiative Dobler 17.410 of 7 March 2017. The initiator proposes an amendment to Art. 242 DEBA.

73 See section 5.2.

74 See section 5.1.

75 See section 5.1.1.

76 See Seiler/Seiler 2018: 149 et seq.; Graham-Siegenthaler/Furrer 2017: margin no. 69; see also Hauser-Spühler/Meisser 2018: 9, distinguishing tokens from data, without however granting them the status of property.

77 See von der Crone/Kessler/Angstmann 2018: 339-340.

78 See the references above in n. 62 et seq.

79 See Seiler/Seiler 2018: margin no. 33.

80 See e.g. Bärtschi/Meisser 2015: 141; Eggen 2018: 561 et seq.; Essebier/Bourgeois 2018: 579; Hauser-Spühler/Meisser 2018: 9; Hürlimann-Kaup 2018: 142 et seq.; Hess/Spielmann 2017: 195-196; Gless / Kugler / Stagno 2015: 90; Gobat 2016: 1098; Maurenbrecher/Meier 2017: margin no. 20; Meisser/Meisser/Kogens

5.1.2 Legal classification of tokens by content[81]

5.1.2.1 General principles

In its guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) published 16 February 2018,[82] FINMA undertook a first official classification of tokens for the sole purpose of financial market law. In order to classify tokens under civil law, it is decisive which legal relationships form the basis for the issue and trade of tokens. A token as such merely constitutes an entry in a decentralised register and thus has no legal effect. Legal obligations arise only between persons who use tokens and attach a legal significance to this action. This means that the circumstances of the individual case are very important for the classification.

The cryptocurrencies that are well-known to the public, such as Bitcoin, fall into the category of "payment tokens". They are designed as a means of payment and generally do not give rise to claims against a particular issuer.[83] They are intended to enable users to acquire goods or services in a given system and thus embody a value recognised within that system. The widespread cryptocurrencies can also be used to acquire analogue goods and services and achieve an objectively determinable market value through trading on exchanges.

In the normal case of an ICO, in contrast, an issuer accepts funds or cryptocurrencies and issues tokens in return. The token is linked to the promise of consideration, which may take on very different forms.[84] Depending on their economic function, FINMA subdivides such tokens into "utility tokens" (which are intended to provide access digitally to an application or service) and "asset tokens" (which are intended to represent assets such as shares in real values, companies, earnings, or debt securities, such as dividends or interest payments).[85] In these cases, the classification of tokens under civil law is determined by the rights and obligations of the acquirer according to the intention of the parties.

In summary, a token issue is intended to link values or rights with an entry in a digital register.[86] The following section examines which values and rights may in theory be considered for such a link and which rules must be observed under current law.

5.1.2.2 Claims

In the normal case of an ICO, the issuer of the token and the acquirer of the token enter into a bilateral contractual relationship, whereby the acquirer of a token undertakes to make a payment (in government-issued money or cryptocurrency) and in return acquires a token (or the promise of a token) which is intended to represent consideration. From a legal point of view, the acquirer of the token in most cases has a claim against the issuer, whereby this claim is linked to a token by means of a contractual agreement and is intended to be asserted by means of this token according to the intention of the parties.

The starting point for the assessment of this procedure is the principle of freedom of contract, in particular the freedom of the terms of the contract: the terms of a contract may be freely determined within the limits of the law.[87] Within the limits of mandatory law, the parties are free

---

2018: margin no. 5-6; Müller/Reutlinger/Kaiser 2018: 86-87; von der Crone/Kessler/Angstmann 2018: 339-340; Weber 2015: 30; Zellweger Gutknecht 2018: 20 et seq., 25.

81 This chapter is concerned with the classification of tokens under civil law. A detailed economic classification and the supervisory treatment of tokens will follow in section 6.2.

82 See FINMA 2018a.

83 See FINMA 2018a: 3; Blockchain Taskforce 2018b: 7.

84 See section 3.2.

85 See FINMA 2018a.

86 On the special case of virtual means of payment as intangible assets, see section 5.1.2.5 below.

87 Art. 19 para. 1 CO.

to agree what they want. The freedom of the terms of the contract also includes freedom of types: the parties are not bound by the types of contracts that are set out by law, but may deviate from them and create new types of contracts ("innominate contracts").[88] Mixed contracts, which combine elements of different types of contract, are common.[89]

An ICO may typically contain elements of the following contract types, depending on how it is structured; it is very important to look at the individual case, however, and the relevant provisions are often applicable only analogously:

- Loan
- Agency contract
- Bailment
- Contract for work and services
- Sale/exchange

When assessing the type of the contractual relationship, it is not decisive how the parties describe their contract; rather, the content of the agreement is decisive, i.e. the true and common intention of the parties.[90] With regard to the question as to which mandatory provisions are applicable to an innominate contract, the interests set out in the contract and the protective purpose of the applicable norm are decisive.[91]

This means that prima facie, the parties may link claims to tokens. However, the *principle of the relativity of contracts* must be taken into account:[92] in a first step, such an agreement binds only the contracting parties themselves. The transfer of claims associated with tokens will be examined in a later step.[93]

5.1.2.3 Membership in a company

a) Limits on company structure

The term "*membership*" under Swiss private law refers to membership of one of the company forms set out by law. Swiss law not only provides for a closed number of companies (formal constraint), but also restricts their content (formal determination). However, the law provides leeway for individual structuring of the specified company forms, in light of the fact that the legislative power has refrained from binding the forms strictly to a legislative model or type under mandatory law.[94]

Under current law, however, it is not permissible to create a hitherto unknown form of membership of one of these company forms through mere ownership of a token within the framework of private autonomy and the freedom of contract. This would exceed the mandatory limits of the freedom to structure companies. In other words, membership of companies is governed exhaustively:

88 See Schwenzer 2016: margin no. 26.21.
89 Schwenzer 2016: margin no. 3.16.
90 Art. 18 para. 1 CO.
91 Schwenzer 2016: margin no. 26.24; Amstutz/Morin 2015: Vor Art. 184 et seq. margin no. 32.
92 See Schwenzer 2016: margin no. 4.06.
93 See section 5.1.4.
94 See Meier-Hayoz/Forstmoser/Sethe 2018: § 11 N 2 and N 4; Forstmoser 2005: 79-80 and Weber 1998: 80 et seq., especially 85-86.

- In the case of companies structured as a legal community such as simple partnerships,[95] general partnerships,[96] and limited partnerships,[97] only persons who also become partners can become members. The creation of one of the aforementioned partnerships does not depend on the mere acquisition of a token as part of an ICO, but rather requires deliberate cooperation by the partners with the aim to establish a partnership. It requires an "*animus societatis*", i.e. the intention to pursue a common purpose by common effort or means, to participate in the decisions of the partnership and to share in profits and losses.[98] Membership in companies structured as a legal community cannot in principle be transferred by way of a legal transaction, given that – in light of the fact that legal communities rely on their personal composition – a change in membership might result in an unreasonable change to the preconditions of cooperation for the participants.[99] The entry or withdrawal of a partner is possible only if the partnership agreement is amended or supplemented at the same time, or if all other partners agree.[100]
- In the case of incorporated companies such as companies limited by shares,[101] partnerships limited by shares,[102] and limited liability companies,[103] membership is not associated with the holding of a token, but rather with the ownership of a share or a capital contribution, which is issued in accordance with a process that is clearly and conclusively set out by law (e.g. the establishment of a company or a capital increase requires a share subscription and fully paid-up capital, possibly a written agreement on contributions in kind, a written incorporation report, a written audit report by a licensed auditor, and a public deed as well as an entry in the commercial register).[104] It is possible to transfer the company share and thus the membership, but this must be done in accordance with the articles of association (e.g. restricted transferability) or contractually (e.g. binding partnership agreements), and the legal reporting, register, and retention requirements must also be met.

b) Possibility of linking tokens to membership of a company

The question can be raised whether tokens can be linked to membership in a company. From the point of view of contract law, this is unobjectionable.[105] Company law likewise does not give rise to specific obstacles, as long as the mandatory limits on company structure are not exceeded.[106] But this does not mean that the mere transfer of a token also leads to the transfer of membership in the company in question. To accomplish this, the existing rules on the transfer of shares must be taken into account, which depend on the legal form of the

95 Art. 530 et seq. CO.
96 Art. 552 et seq. CO.
97 Art. 594 et seq. CO.
98 See BGE **127** III 519 E. 2d.
99 See Meier-Hayoz/Forstmoser/Sethe 2018: § 2 N 101, § 3 N 34, although other contractual arrangements may be made.
100 See BGE **134** III 577 E. 3.3; but it is possible to provide for facilitations in the partnership agreement.
101 Art. 620 et seq. CO.
102 Art. 764 et seq. CO.
103 Art. 772 et seq. CO.
104 Müller/Stoltz/Kallenbach 2017: 1327 et seq.
105 See section 5.1.2.2 on the principle of freedom of contract.
106 See section 5.1.2.3.

company.[107] Moreover, the linking of a token to membership in a company is binding only on the parties and cannot be asserted against a third party.[108]

5.1.2.4 Rights in rem

a) Principle: Embodiment of rights in rem through ownership

Rights in rem are considered absolute rights, i.e. they can be asserted against anyone. Similarly to company law but in contrast to contract law, the principles of constrained type and determination of type apply in property law.[109] The law provides for an exhaustive number of rights in rem, the content of which is largely predetermined.[110]

According to the prevailing doctrine, rights in rem are personal rights which give the entitled party direct sovereignty over property and the authority to exclude third parties from it.[111] The prototype is the right of property. Since rights in rem can be asserted against anyone, they should also be recognisable to everyone (principle of publicity).[112] As a rule, publicity is fulfilled by the possession of the object.

In exceptional cases, register entries may fulfil the principle of publicity (and thus replace possession).[113] Examples include the land register for land ownership,[114] the register for the pledge of livestock,[115] ships,[116] aircraft,[117] and the reservation of ownership.[118] But these are exceptions provided by law. These registers provided by law are maintained by official bodies. Tokens can therefore, as a rule, not represent objects and not represent rights in rem with legal effect.[119]

b) Separation of ownership and direct possession

As demonstrated above, ownership is usually expressed by possession of an object or – in a few exceptions provided by law – by entry in a register. However, there are constellations in which someone is the owner who does not directly possess and effectively control an object, for example when a third party holds the object in safe custody for the owner. In such cases, the owner's possession is said to be indirect and that of the custodian to be direct. It is also conceivable that ownership refers only to a part of the object and that the object is held in safe custody for several co-owners.[120]

Co-ownership may also arise if movable property (chattel) of different owners is held in joint custody and mixed together.[121] According to case law and theory, the collective safe custody of securities already entailed co-ownership shares in the total portfolio of the collective custody account prior to entry into force of Article 973a CO; this is referred to as modified, unstable co-

---

107 For example, the transfer of membership in a company limited by shares is guaranteed if the membership is securitised by a bearer share or ordinary registered share, because in these cases – broadly speaking – the handing over of the certificate or compliance with formal requirements such as endorsement is sufficient to execute a change of membership that is effective vis-à-vis the company limited by shares (see Meier-Hayoz/Forstmoser/Sethe 2018: § 3 N 71); on the transfer of tokens in general, see section 5.1.4 below.

108 See section 5.1.2.2 on linking claims to tokens.

109 Hrubesch-Millauer/Graham-Siegenthaler/Roberto 2017: margin no. 01.63 et seq.

110 Rey 2007: margin no. 6 et seq.; Hrubesch-Millauer/Graham-Siegenthaler/Roberto 2017: margin no. 01.63 et seq.

111 Rey 2007: margin no. 200 and other references.

112 Rey 2007: margin no. 272 et seq.

113 See Hrubesch-Millauer/Graham-Siegenthaler/Roberto 2017: margin no. 01.56.

114 Art. 937 para. 1 CC.

115 Art. 885 CC.

116 Federal Act on the Shipping Register; SR **747.11**

117 Federal Act on the Aircraft Register; SR **748.217.1**

118 Art. 715 CC.

119 See Eggen 2017a: 10 et seq.; for exceptional constellations, see section 5.1.2.4 b) below.

120 Art. 646 para. 1 CC.

121 Art. 727 para. 1 CC.

ownership.[122] The creation of co-ownership shares in money is ruled out:[123] the mixing together of money entails the sole ownership by the party in direct possession of the money; the former owners merely have a contractual right to reimbursement of the sum paid in.

The legal construct of constructive possession also allows co-ownership to be established without the co-owner ever having been in direct possession of the object. This occurs where the seller of an object – or parts thereof – remains in direct possession of the object on the basis of a legal transaction agreement.[124] In this case, the co-ownership share is established by several legal transactions: the contract of possession, the underlying legal transaction for the transfer of ownership, and the legal transaction on the basis of which the object remains in the direct possession of the seller.[125] Any formal requirements must be observed in this regard: for example, a public deed and entry in the land register are required for the establishment of co-ownership of real estate.[126] In individual cases, it will also have to be examined carefully whether the intention of the parties actually aims to create a co-ownership share in rem or whether the purpose is instead the conclusion of a tradable contract on the *value* of an object.[127]

c) Conclusion

Because rights in rem are exercised by way of possession of the legal object, tokens as a rule are not able to represent property and accordingly rights in rem in a legally effective way.

In cases where rights in rem exist through indirect possession and contractual agreement between the party with direct possession and the owner, however, representation of these rights in a decentralised register such as a blockchain appears conceivable prima facie. This is always the case when an object is held in safe custody by a person who is not the owner and no special form is prescribed for the underlying legal transactions. Whether rights in rem can also be transferred in this way will be examined in section 5.1.4.3 below.

5.1.2.5 Cryptocurrencies

a) Intangible assets

The first and best-known example of a token – Bitcoin – as well as other cryptocurrencies represent a special case for legal classification. Unlike most ICOs, there is no issuer in such cases who issues tokens in exchange for capital.[128] There is accordingly no legal relationship between the issuer and the acquirers of tokens that could be qualified as a claim or membership relationship. Consequently, the value of such tokens cannot be measured according to a legal position mediated by it.

Cryptocurrencies are based on the consent of their users.[129] Only sporadically, however, is it argued that such tokens confer a right of claim in the form of a claim for recognition directed against all other system participants in the blockchain:[130] according to this opinion, each participant in a blockchain submits to the rules defined according to the respective blockchain protocol governing how tokens are held and transferred. This creates a contractual relationship with all other participants in the system, giving the holder of a token a right of recognition against the totality of the participants in the system. According to this view, the obligee of the

---

122 BGE **112** II 406 E. 4; Rey 2007: margin no. 639-640 and 1941 et seq.; Kuhn 2016: Art. 973a OR: margin no. 6.
123 BGE **136** III 247 E. 5 and other references; Rey 2007: margin no. 1943-1944 and other references.
124 Art. 924 para. 1 CC; see Schmid/Hürlimann-Kaup 2017: margin no. 178 et seq.
125 Schmid/Hürlimann-Kaup 2017: margin no. 184; on the transfer of possession through a legal transaction, see also section 5.1.4.3.
126 Art. 656-657 CC.
127 On derivatives, see section 6.4.2.
128 See e.g. the references in n. 83.
129 See Müller/Reutlinger/Kaiser 2018: 81; Zellweger Gutknecht 2018: 24-25.
130 See von der Crone/Kessler/Angstmann 2018: 340-341.

right of recognition is the owner of the token, while all other participants in that blockchain are the obligors.

It is an open question, however, whether the assumption of legal relationships among blockchain users solely in virtue of participation in a blockchain system does justice to the actual circumstances in a "trustless, decentralised system", as the Bitcoin blockchain in particular represents. The "rules" of the blockchain protocol are algorithmic in nature and addressed to computers that use cryptographic processes to ensure the integrity of the blockchain. While blockchain tokens may have a value that results from the interplay of supply and demand, it is difficult to imagine that a claim in the sense of a potentially enforceable right to performance against any other participant can be derived from this fact. As a rule, it is questionable whether the individual users have the intention to bind themselves legally in this way.[131] Classification of cryptocurrencies as claims accordingly also contradicts FINMA's practice in regard to cryptocurrencies and the Federal Council's report on virtual currencies.[132]

Most probably the prevailing doctrine classifies cryptocurrencies as *intangible assets*.[133] According to this doctrine, they represent algorithmically secured, purely *de facto* assets. Even though these values do not themselves constitute claims, they are nevertheless amenable to contractual agreements. In the following discussion, we will examine how these cryptocurrencies are to be classified when they are made the object of a contractual agreement.

b) Money?

The Swiss legal system does not define money clearly, uniformly or systematically.[134] This is why the legal qualification of virtual currencies – or more specifically Bitcoin – as money has only a limited scope.

Doctrine distinguishes between money in the broader sense and money in the narrower sense. Money in the narrower sense refers to all the means of payment listed in Article 2 of the CPIA[135], i.e. the coins issued by the Confederation (lit. a), the banknotes issued by the Swiss National Bank (lit. b) and Swiss franc sight deposits with the Swiss National Bank (lit c).[136] This definition does not include cryptocurrencies (e.g. Bitcoin), or cheques, bills of exchange, credit cards, book money (scriptural money) and electronic money (e-money).[137] In the broader sense, doctrine recognises a functional definition of money, on which most provisions of the Civil Code and the Code of Obligations are based, but without making this the rule. It is generally believed that money fulfils three functions: first, it is a unit of account; second, a means of exchange or payment; and third, a store of value.[138] The Federal Council adopted this definition in its 2014 report on virtual currencies.[139] According to prevailing doctrine, however, the most significant of the three is as a means of exchange or payment for goods or

131 See Eggen 2018: 561; Hess/Lienhard 2018: 158; Bärtschi/Meisser 2015: 143-144; Gobat 2016: 1098; Maurenbrecher/Meier 2017: margin no. 21; Müller/Reutlinger/Kaiser 2018: 86-87.
132 See Report on Virtual Currencies: 14.
133 See Eggen 2018: 562-563; Gobat 2016: 1098-1099; Müller/Reutlinger/Kaiser 2018: 86-87.
134 Bärtschi/Meisser, 2015: 142; Leu 2015: Art. 84 CO N 1; Mercier 2016: Art. 84 CO N 3.
135 SR **941.10**
136 See Art. 2 of the Federal Act of 22 December 1999 on Currency and Payment Instruments (CPIA; SR *941.10*); Loertscher 2012: Art. 84 CO N 6; Schönknecht 2016: 308.
137 Bärtschi/Meisser2015: 142 et seq.; Hauser/Meisser 2018: 6 et seq., 7; Leu 2015: Art. 84 N CO 2; Loertscher 2012: Art. 84 CO N 6; Mercier 2016: Art. 84 CO N 3; Schönknecht 2016: 308.
138 Beck 2015: 580 et seq., 582 et seq.; Eggen 2017b: paras. 5-8; Gless/Kugler/Stagno 2005: 82 et seq., 83; Weber 2005: Art. 84 CO N 13-15; Hess/Lienhard 2018: 157.
139 Report on virtual currencies: 7. However, the definition of "money" in the glossary (p. 29) is narrower in that it has to be "generally accepted by the public".

services.[140] According to some, this criterion should be decisive also if a means of payment is issued by private individuals or only traded in a small circle.[141]

As the functions described above are – at least partially – fulfilled by cryptocurrencies, it is generally accepted that they fall under the broadest sense of the term money.[142] They are primarily a unit of account with which a price can be expressed.[143] They can be the subject of a contractual commitment by a party wishing to pay for goods or services in a cryptocurrency.[144] In principle, it is sufficient for the creditor to accept this currency and for the transaction to take place via the respective register, whereby the intent of the contracting parties must be precisely determined in each individual case, especially in the event of difficulties in contract execution.[145] Finally, most cryptocurrencies can be exchanged for national currencies on corresponding platforms, although their exchange rates can vary significantly.[146] Nevertheless, it cannot be concluded here that cryptocurrencies belong absolutely to "money" in the broader sense. Each specific provision surrounding the term must be interpreted in order to determine whether or not it includes the cryptocurrency in question.[147]

With regard to Bitcoin, the Federal Council concluded in its 2014 report on virtual currencies that although this cryptocurrency fulfils the above-mentioned functions of money to a certain extent, it cannot be recognised as such because of its high volatility relative to official currencies.[148] Many do not share this view.[149] However, this has no civil law effect on transactions with Bitcoins, which are covered by Article 1 of the CO provided the condition of mutual expression of intent by the parties is fulfilled.[150] Consequently, it is necessary to determine in the individual case and according to the parties' intent whether payment can be made with a cryptocurrency and how this payment is to be qualified.

5.1.3 Classification by wrapper: Negotiable securities, uncertificated securities, and intermediated securities

5.1.3.1 Background

According to the intention of many users, the blockchain as a decentralised register should be able to represent rights and make them tradable. It would therefore make sense to classify the blockchain under securities law. When rights are securitised, values (rights) are attached to a paper instrument.[151] The rights are wrapped into a special form and are therefore subject to special rules, affecting their transfer in particular (see section 5.1.4). The attachment of a right to an object has traditionally made the rights amenable to circulation and capital markets.[152] The rights are mobilised by their embodiment in an instrument.

---

140 Bärtschi/Meisser 2015: 142; Gless/Kugler/Stagno: 2005: 82 et seq., 83; Schönknecht 2016: 308; Weber 2005: Art. 84 CO N 13, N 15, N 65-67. Implicitly see also Piller 2017: 1426 et seq.

141 Bärtschi/Meisser 2015: 142; Piller 2017: 1428. On the controversy regarding the need for state issuance of money: Weber 2005: Art. 84 CO N 25.

142 Bärtschi/Meisser 2015: 143; with caution Eggen 2017b: para. 12 et seq.; Hauser/Meisser 2018: 6 et seq., 7; Piller 2017: 1428; Schönknecht 2016: 309. Corresponds to FINMA practice, see Art. 2 lit. c of the AMLO-FINMA, according to which virtual currencies can also be the subject of money and asset transfers just like cash, precious metals, cheques or other means of payment.

143 Beck 2015: 585.

144 Bärtschi/Meisser 2015: 145; Eggen 2017b: para. 15.

145 Eggen 2017b: para. 15 et seq.; Hauser/Meisser 2018: 7.

146 Gless/Kugler/Stagno 2005: 82 et seq., 87; Schönknecht 2016: 309.

147 Eggen 2017b: para. 5; Piller 2017: 1428.

148 Report on virtual currencies: 10. In the same vein: Weber/Takacs 2018: 37 et seq.

149 For instance, Hauser/Meisser 2018: 7; Gless/Kugler/Stagno 2005: 82 et seq., 87-88; Piller 2017: 1428; Schönknecht 2016: 309.

150 Report on virtual currencies: 10. Contra Bärtschi/Meisser 2015: 144.

151 See Meier-Hayoz/von der Crone 2018: margin no. 1 et seq.; Dispatch regarding FISA, 9321.

152 Meier-Hayoz/von der Crone 2015: margin no. 1315.

According to the legal definition, negotiable securities are instruments to which a right attaches in such a manner that it may not be exercised or transferred without the instrument.[153] They fulfil various functions:[154]

- Proof of entitlement: Possession of the security serves as proof of entitlement to assert the securitised right.
- Transfer: Transfer of possession of the paper instrument is a prerequisite for transfer of the securitised right.
- Protection of transactions: Possession of the paper instrument is the basis for the protection of *bona fide* acquirers of securities of public faith.

Figuratively speaking, securities law wraps a "mere" right in a special legal framework that serves to simplify proof of entitlement, transfer, and protection of transactions.[155]

In the course of technological progress and digitalisation, however, there has for some time been a trend towards immobilisation and ultimately dematerialisation of securities.[156] The instruments, which originally were mobile, have increasingly been stored in centralised locations by custodians and thus immobilised. The embodiment of rights in instruments has increasingly been perceived as an obstacle to trading. In many cases, physical instruments are no longer issued at all. As part of this development, the new categories of uncertificated securities[157] and intermediated securities[158] have been created.

The following discussion will examine where tokens should be situated within the existing categories of securities law.

5.1.3.2 Certificated securities

a) Definition and creation of certificated securities

As mentioned above, securities are instruments (certificates) to which a right attaches in such a manner that it may not be asserted or transferred without the instrument.[159] In securities law, there is no legal definition of what is meant by an instrument. In contrast, a legal definition of the equivalent terms "official document" or "physical record" can be found in both criminal law[160] and the law of civil procedure.[161] According to these definitions, written works, indications, recordings and the like that are suitable to prove legally significant facts are considered to be official documents or records. In criminal and civil procedural law, however, the emphasis is on the function of these documents as evidence. The definition of an official document is therefore ill-suited for the purposes of securities law,[162] given that evidential value is only one of the functions a negotiable security is intended to fulfil. Moreover, a separate

153 Art. 965 CO.
154 See the summary in the Dispatch regarding FISA, 9321 et seq.
155 See Zobl/Gericke 2013: Syst. Teil BEG: margin no. 17.
156 Dispatch regarding FISA, 9321 et seq.
157 See section 5.1.3.3.
158 See section 5.1.3.4.
159 Art. 965 CO.
160 Art. 110 no. 4 SCC.
161 Art. 177 CPC.
162 Furter 2012: Vor Art. 965-1155 OR N 2.

definition of the equivalent term "public deed" exists with respect to public certification.[163] Work to introduce public deeds in electronic form is underway.[164]

Even under securities law, it at least appears undisputed that an instrument does not necessarily mean a sheet of paper. In the theory of securities law, instruments are defined as written works containing a declaration relevant to private law[165] or written works that express (legally relevant) thoughts.[166] The carrier of such a declaration and an associated expression of intent (or a written element that entails an expression of intent) are the crucial elements that have been identified by legal theory.[167] The declaration and the carrier of that declaration must be durably, but not inseparably, connected with each other.[168] The academic literature also recognises as documents storage media containing an electronic record of a declaration.[169] It is argued that even in the case of storage media, the declaration is sufficiently durably connected with the carrier of the declaration.[170] But it must be noted that for certain types of securities, a signature in one's own hand or at least a replica of the signature is required by law, for example in the case of share certificates,[171] documents of title to goods,[172] as well as cheques and bills of exchange.[173]

A carrier of a declaration becomes a negotiable security through agreement on a certificate clause. This clause stipulates that the performance owed may or must be validly provided only upon presentation of the instrument (bilateral presentation clause or simple securities clause). Furthermore, it may be agreed that the party presenting the instrument shall be deemed to have legal competence (bilateral proof-of-entitlement clause or qualified securities clause).[174] The negotiable security is created through the issuance of the instrument and contractual agreement on the certificate clause. This agreement is referred to as a transfer agreement for negotiable instruments.[175] The securitised right may either already exist or be newly created with the transfer agreement. The transfer agreement is not expressly governed by Swiss law; it should be presumed that it may also be concluded tacitly.

b) Securitised rights

In principle, all contractual claims are amenable to securitisation. In the case of memberships under company law, securitisation is possible only where the law permits, which is currently the case only for companies limited by shares and partnerships limited by shares.[176] A corresponding *numerus clausus* also exists in property law, where securitisation of rights in

---

163 See the definition of the term "public deed" in Art. 55 of the Final Part of C-CC set out in the consultation proposal of the Federal Council of December 2012 (available at: https://www.admin.ch/ch/d/gg/pc/documents/2215/ZGB_Oeffentliche-Beurkundung_Entwurf_de.pdf; visited on 7 September 2018): "Recording of statements or legally relevant facts relating to legal transactions or proceedings, by a local notary public competent in regard to the subject matter, in a document in a prescribed form and according to a prescribed procedure".

164 See press release by the Federal Council of 25 May 2016. Available at: www.bj.admin.ch > Latest News > News > 2016 (as at 18 October 2018).

165 See e.g. Meier-Hayoz/von der Crone 2018: margin no. 6; Kuhn 2016: Art. 965 N 19, and other references in each.

166 See Petitpierre-Sauvain 2006: 15.

167 Meier-Hayoz/von der Crone 2018: margin no. 6; Furter 2012: Vor Art. 965-1155 OR N 2.

168 Meier-Hayoz/von der Crone 2018: margin no. 7; Furter 2012: Vor Art. 965-1155 OR N 5.

169 Meier-Hayoz/von der Crone 2018: margin no. 8-9; Furter 2012: Vor Art. 965-1155 OR N 3; Kuhn 2016: Art. 965 N 20 OR.

170 Meier-Hayoz/von der Crone 2018: margin no. 8.

171 Art. 622 no. 5 CO.

172 Art. 1153 no. 1 CO.

173 Art. 991 no. 8 CO, Art. 1096 no. 7 CO and Art. 1100 no. 6 CO.

174 Kuhn 2016: Art. 965 N 6. et seq.

175 See Meier-Hayoz/von der Crone 2018: margin no. 261 et seq.

176 Furter 2012: Vor Art. 965-1155 OR N 10.

rem is possible only in the case of mortgage certificates[177] and bonds secured by a mortgage right.[178/179] In the case of documents of title to goods, the right in rem to the goods themselves is not securitised, but rather the contractual right to surrender of the goods.[180] According to a common definition, a document of title to goods is an "acknowledgement of receipt, in the form of a negotiable security, of goods received from a third party, with the obligation to surrender the goods only to the legitimate holder of the document".[181] Nevertheless, transfer of the document of title to goods can be used to transfer ownership of the goods, since indirect possession of the goods is transferred together with the document.[182]

c) Effects of securitisation

The certificated security has different effects depending on the agreement. A distinction is made between securities of public faith (bearer securities and order instruments) and registered securities:[183]

- *Registered securities*: The performance owed may or must be validly provided only upon presentation of the instrument (bilateral presentation clause or simple securities clause)
- *Securities of public faith*: The performance owed may or must be validly provided only upon presentation of the instrument (bilateral presentation clause or simple securities clause). In addition, the party presenting the instrument is deemed to have legal competence (bilateral proof-of-entitlement clause or qualified securities clause). A distinction is made between two subtypes of instruments of public faith:
  - *Bearer securities (e.g. bearer shares)*: The bearer of the instrument is deemed to have legal competences.
  - *Order instruments (e.g. registered shares)*: The bearer of the instrument – whom the instrument also names as the authorised party or the legal successor of the authorised party – is deemed to have legal competence. Legal succession is indicated by the chain of endorsements on the back of the instrument.

In the case of securities of public faith, a protection of transactions applies, which traditionally was intended to make them capable of circulation. Acquirers of a securitised right are protected in their faith in the power of disposition of the seller and in the securitised right.[184] As in the case of rights in rem, the basis of this faith is publicity.[185] Legal competence as well as the content of the securitised right should be recognisable from the outside, which is why one can rely on it in trading. This protection of transactions is even more extensive in the case of *bearer securities* than in the case of chattel. While an object cannot be acquired by an unauthorised person if it has been lost to the original owner against that owner's will,[186] the acquisition by a *bona fide* acquirer of bearer securities is also protected in such cases.[187] With regard to the

177 Art. 842 et seq. CC.
178 Art. 875 CC.
179 Meier-Hayoz/von der Crone 2018: margin no. 11 et seq.; Furter 2012: Vor Art. 965-1155 OR N 8.
180 Meier-Hayoz/von der Crone 2018: margin no. 1512.
181 Oftinger/Bär 1981: Art. 902 N 4; see also Christen/Hauck 2012: Art. 1153-1155 OR N 1; Ernst 2016: Art. 925 ZGB N 2.
182 See Ernst 2016: Art. 925 ZGB N 3; for details, see section 5.1.4.3 below.
183 Meier-Hayoz/von der Crone 2018: margin no. 253.
184 See Meier-Hayoz/von der Crone 2018: margin no. 326 et seq.
185 See section 5.1.2.4.
186 Art. 934 CC.
187 Art. 935 CC.

content of the securitised right, a limitation of objection applies.[188] The party obliged under the instrument is in principle liable for the estoppel created by the instrument.[189]

Above all, the securitisation of rights also has an impact on the transfer of these rights. In principle, such transfer is effected under the rules of property law and no longer under the rules that would be applicable to the securitised right.[190]

d) Tokens as certificated securities *de lege lata*?

In the Blockchain Taskforce's position paper on the legal classification of ICOs, the view is expressed that tokens can be classified as certificated securities in a teleological interpretation of the concept of securities.[191] Tokens are accordingly classified together with the blockchain (as a publicly accessible database) as carriers of declarations.[192] In this view, tokens are suitable for recording a declaration and are durably connected with the blockchain. The blockchain thus performs the same function as a conventional electronic or paper instrument. Tokens contain a bearer clause, given that it is evident that only the bearer of the *private key* can assert the right "securitised" in the token.[193] Finally, this view holds that possession of a token and thus the transfer of possession is possible, given that these terms are to be understood digitally according to a teleological interpretation.[194] Like a party in possession of an object, the bearer of a *private key* exercises actual power over a token. Already in the position paper, however, it is pointed out that this interpretation is associated with legal uncertainty. In its *white paper*, the Blockchain Taskforce indeed refrains from endorsing this position, due to a "lack of legal certainty and judicial practice."[195]

It is in fact uncertain whether a court would agree with this view. It is already questionable whether in the case of a token, a declaration can actually be assumed to be associated with a carrier. As a rule, a token consists solely of an entry in a digital register, and there are accordingly not two different elements connected with each other. It is also questionable whether – contrary to the prevailing doctrine – the rules of possession can actually be interpreted digitally and whether the element of physicality can thus be dispensed with. As has already been discussed with regard to the legal classification of data, the element of physicality continues to be key to property law in its current form.[196] Securities law is similarly based on the notion that certificated securities are tangible objects embodying or objectifying rights.[197] In other words, the special rules of securities law are based on the linking of a non-physical right with a physical object. The concept of a security thus does not appear readily available to digitalisation.[198]

---

188 Art. 979 CO; Art. 1146 CO.
189 See Meier-Hayoz/von der Crone 2018: margin no. 366.
190 See section 5.1.4.3.
191 See Blockchain Taskforce 2018b: 6 et seq.; similarly, see also Weber/Iacangelo 2018: margin no. 7 et seq.
192 Blockchain Taskforce 2018b: 6-7.
193 Blockchain Taskforce 2018b: 8.
194 Blockchain Taskforce 2018b: 10-11.
195 Blockchain Taskforce 2018a: 21.
196 See section 5.1.1.1 and section 5.1.2.4.
197 See section 5.1.3.1
198 See von der Crone/Kessler/Angstmann 2018: 341; see also Kuhn 2016: Art. 965 OR N 15: "According to the Swiss understanding of the law […] possession is possible only with respect to a physical carrier of a declaration (CC 919 I). While it is certainly conceivable to place the functions of securities pertaining to proof of entitlement, transfer, and protection of transactions on a different basis – in particular book entries with the borrower or issuer – it is doubtful whether this development can be managed without the intervention of the legislative power solely by further development of the law through practice."

5.1.3.3 Uncertificated securities

a) Definition and creation of uncertificated securities

According to the legal definition, uncertificated securities are rights with the same function as negotiable securities.[199] This definition does not say much, however.[200] The criterion of the "same function as negotiable securities" is not very helpful, since the functions of negotiable securities (proof of entitlement, transfer, protection of transactions) depend significantly on securitisation, i.e. the physical embodiment of a right in an instrument.[201]

The conditions under which rights can be structured as uncertificated securities are not explained in more detail in the law. The borrower may replace existing, fungible negotiable securities or global certificates that have been entrusted to a single bailee with uncertificated securities or issue rights as uncertificated securities from the outset. In principle, it can be assumed that all rights that can be securitised can also be issued as uncertificated securities if the conditions for issue or the articles of association of the borrower so provide or if the bailors (or creditors)[202] have given their consent.[203] In securities theory, it is sometimes argued that bearer shares can also be issued in the form of uncertificated securities, although uncertificated bearer shares would seem to be a contradiction in terms.[204] This has to do with the fact that, according to the case law of the Federal Supreme Court, the membership securitised in a bearer security still exists if, for example, the share was not issued or the security was destroyed.[205] It is disputed whether the rights must be fungible in order to be issued as an uncertificated security. Some of the literature affirms this by analogy with the collective custody of negotiable securities.[206] Other authors take the opposite view.[207] Because tokens are generally intended to embody fungible rights, however, the question is not crucial in this context.

An uncertificated security is created with an entry in an uncertificated securities register of the borrower.[208] This register is usually maintained electronically and is not public. It may also arise from the borrower's accounting. The uncertificated securities register provides information on the number and denomination of the uncertificated securities issued as well as the first creditors. It is not mandatory that the uncertificated securities register be updated.

b) Effects of design as an uncertificated security

When the design as an uncertificated security is chosen, claims and other rights are dressed up as negotiable securities, so to speak.[209] They retain their contractual nature, however.[210] Uncertificated securities are lacking components under property law.[211] This means they in

---

199 Art. 973*c* para. 1 CO.
200 Dispatch regarding FISA: 9328; Eggen 2009: 117; Pöschel/Maizar 2012: Art. 973*c* OR N 23 et seq.; Bohnet/Hänni 2017: Art. 973c N 5.
201 See Pöschel/Maizar 2012: Art. 973*c* OR N 29 et seq.; Kuhn 2016: OR 973c N 1b.
202 See Pöschel/Maizar 2012: Art. 973*c* OR N 17 with a reference to the unfortunate wording of the law in this regard.
203 Art. 973*c* para. 1 CO; Bösch 2013: Art. 973c OR N 5; Pöschel/Maizar 2012: Art. 973*c* OR N 42.
204 Lanz/Favre 2009: 549; Bösch 2013: Art. 973*c* OR N 6; Pöschel/Maizar 2012: Art. 973*c* OR N 36; for an opposing view, see Böckli 2009: § 4 N 124.
205 BGE **83** II 445 E. 4
206 Art. 973*a* CO; Pöschel/Maizar 2012: Art. 973*c* OR N 25; Bohnet/Hänni 2017: Art. 973c OR N 5; Bösch 2013: Art. 973*c* N 5; see also von der Crone/Kessler/Angstmann 2018: 342-343.
207 Bärtschi 2013: Art. 6 BEG N 52; Furter 2014: Art. 973*c* N OR 6.
208 Art. 973*c* para. 3 CO.
209 Pöschel/Maizar 2012: Art. 973*c* OR N 42.
210 Pöschel/Maizar 2012: Art. 973*c* OR N 43; Bohnet/Hänni 2017: Art. 973c OR N 4; Meier-Hayoz/von der Crone 2018: margin no. 1326.
211 Meier-Hayoz/von der Crone 2018: margin no. 1326; Bohnet/Hänni 2017: Art. 973c OR N 4.

principle cannot guarantee publicity and are thus unable to perform the function of the protection of transactions that is performed by securities of public faith.

Since entry into force of the Federal Intermediated Securities Act (FISA), the main function of uncertificated securities has been to serve as a basis for the creation of intermediated securities.[212] But there continue to be uncertificated securities that are not intermediated securities. Various provisions of financial market law refer to uncertificated securities; for instance, standardised uncertificated securities which are suitable for mass trading are considered securities.[213]

c) Tokens as uncertificated securities *de lege lata*

Due to their contractual nature, uncertificated securities are in principle amenable to a contractual link with tokens. Both FINMA and the Blockchain Taskforce assume that a large number of tokens in circulation or planned can be classified as uncertificated securities.[214] The blockchain then performs the function of an uncertificated securities register.[215] This view is also supported by much of securities theory.[216] According to ESSEBIER/BOURGEOIS, the issuance of uncertificated securities would have to be *intentional*, however.[217] These authors argue that there as so few requirements for the issue of uncertificated securities because the intention is to facilitate the creation of intermediated securities. If an issuer of a token does not have the intention to create an uncertificated security, this view holds that tokens should be defined as uncertificated securities only with reservations.[218]

5.1.3.4 Intermediated securities

The Federal Intermediated Securities Act (FISA),[219] which came into force on 1 January 2010, regulates the custody of certificated and uncertificated securities by custodians and their transfer.[220] It applies to intermediated securities that are credited to a securities account by a custodian.[221] According to the exhaustive enumeration in the law, the following are deemed to be custodians: banks, securities dealers, fund management companies, central securities depositories, the Swiss National Bank, Swiss Post, and foreign financial intermediaries that maintain securities accounts in the course of their business activities.[222] Intermediated securities are created when a custodian accepts certificated securities for collective custody and credits them to one or more securities accounts,[223] when a custodian accepts a global certificate for custody and credits the respective rights to one or more securities accounts,[224] or when a custodian registers uncertificated securities in the main register and credits the respective rights to one or more securities accounts.[225] For each issue of uncertificated securities, a single custodian as referred to in Article 4 FISA must maintain the main register.[226] This requirement of a central custodian is likely not easily reconciled with the blockchain as a

---

212 See section 5.1.3.4; Bösch 2013: Art. 973*c* OR N 2.
213 Art. 2 let. b FMIA; Art. 3 let. b FinSA; for details, see section 6 below.
214 FINMA 2018a; Blockchain Taskforce 2018b: 8 et seq.
215 von der Crone/Kessler/Angstmann 2018: 342-343.
216 Eggen 2018: 564; von der Crone/Kessler/Angstmann 2018: 342-343; Hess/Lienhard 2017: margin no. 46-47.
217 Essebier/Bourgeois 2018: 572.
218 Essebier/Bourgeois 2018: 572, 576.
219 SR **957.1**
220 Art. 1 para. 1 FISA.
221 Art. 2 para. 1 FISA.
222 Art. 4 FISA.
223 Art. 6 para. 1 let. a FISA.
224 Art. 6 para. 1 let. b FISA.
225 Art. 6 para. 1 let. c FISA.
226 Art. 6 para. 2 FISA.

decentralised register.[227] Classification of tokens as intermediated securities will therefore generally not be conceivable.

5.1.4 Transfer of tokens

5.1.4.1 General principles

As discussed above,[228] a token is merely an entry in a decentralised register and has no legal effects of its own. However, such an entry can be based on a right that was established through a legal transaction and also exists independently of the link with a token. The question of the legal effects of the transfer of tokens is therefore closely linked to the interpretation of legal transactions. In which cases the parties intend for a right to be transferred together with the transfer of a token can be answered only by interpreting the legal transactions that form the basis of the corresponding right and its transfer. Such an interpretation can be given only on a case-by-case basis and must include all relevant conduct of the parties.[229] The following discussion will therefore limit itself to examining which legal requirements exist for the transfer of rights. The goal is to ascertain when the transfer of a right can take place through an expression of intent that might also be expressed through the transfer of a token. Particular attention will be paid to the limits imposed by current law on the transfer of rights.

As before, the transfer of payment tokens or cryptocurrencies (e.g. Bitcoin) must be considered separately.

5.1.4.2 Simple claims and uncertificated securities

a) Assignment

Claims can be transferred between the old and the new creditor by means of an assignment agreement. The assignment agreement (act transferring entitlement) is valid only if done in writing.[230] The assignment agreement must therefore be signed by the person on whom it imposes obligations,[231] i.e. the assignor.[232] The signature must be appended by hand in principle, but a signature reproduced by mechanical means is recognised as sufficient where such reproduction is customarily permitted.[233] An authenticated electronic signature within the meaning of the Federal Act on Electronic Signatures (ESigA) is deemed equivalent to a handwritten signature.[234] This solution does not appear to be very practical in the blockchain context, however.[235] No particular form is required for the undertaking (act creating a legal obligation) to enter into an assignment agreement.[236]

According to the explicit legal provisions, a written assignment agreement is likewise required for the transfer of uncertificated securities.[237] Already before that provision came into force, the literature argued in favour of applying the law of assignment.[238] If other formalities are envisaged for the transfer of a right constituted as an uncertificated security (e.g. in the case

227 See also Blockchain Taskforce 2018b: 15.
228 See section 5.1.2.1.
229 On the interpretation of declarations of intent, see Schwenzer 2016: margin no. 27.33 et seq.
230 Art. 165 para. 1 CO.
231 Art. 13 CO.
232 Gauch/Schluep/Emmenegger 2014: N 3416; Schwenzer 2016: margin no. 90.13.
233 Art. 14 para. 2 CO.
234 SR **943.03**; Art. 14 para. 2bis CO.
235 Blockchain Taskforce 2018b: 5; von der Crone/Kessler/Angstmann 2018: 343; Eggen 2018: 564.
236 Art. 165 para. 2 CO.
237 Art. 973*c* para. 4 CO.
238 See e.g. Lanz/Favre 2009: 550.

of registered shares with restricted transferability), the prevailing view states that these formalities must be met cumulatively with the formalities of written assignment.[239]

The requirement of written form for the assignment agreement serves to protect the borrower and the course of business.[240] Because only the old creditor and the new creditor are involved in the assignment, the transaction must be clearly documented. Also protected are the creditors of the assignor and of the acquirer, for whom it should likewise be clearly evident when a claim has been transferred.[241]

b) Assumption of contract

In the case of the assumption of a contract, the transferee not only assumes a claim, but also enters into all rights and obligations of the contractual relationship as an obligee and as an obligor. New claims will henceforth arise in the person of the transferee. Assumption of contract is typical for permanent obligations such as tenancy and employment contracts and is in some cases also provided for by law.[242] Assumption of contract is effected by an agreement of all three parties.[243] The law does not explicitly regulate assumption of contract and does not prescribe any form for the agreement effecting it. According to theory and case law, this agreement is *sui generis* and can be concluded without requirements as to form if no form is prescribed for the original contract.[244]

It is questionable whether blanket consent of a party can also be given in advance. For example, an issuer of tokens might declare in advance that it recognises whoever happens to be holding a token as the counterparty and that a transfer of a token should be considered a transfer of contract. It appears that the Federal Supreme Court has not yet dealt with the question of the blanket transfer of contract. The academic literature deems authorisation contained in the contract to be sufficient.[245] In a 2011 judgment, however, the Court of Appeal of the Canton of Zurich did not consider blanket consent in advance to be sufficient.[246] The Court of Appeal deemed the new contracting party to be one of the *essentialia negotii*, which is why the party remaining in the contract would have to *subsequently* agree to the replacement of its contracting party. In the Blockchain Taskforce's position paper on the legal classification of ICOs, the participation of the issuer in the transfer of the contract was deemed impracticable if the transfer took place via a trading platform.[247] A permanent offer in the general terms and conditions for the transfer to any third party was considered to be disputed in contract theory, and the paper also pointed out the problem of the global assumption of general terms and conditions in practice.

With regard to the special case of an ICO, it should also be noted that holders of tokens generally fulfil their part of the contract immediately after or with the conclusion of the contract. The token therefore generally embodies only the counterclaim that is still open, which is to be transferred along with the transfer of the token. This would correspond to the classical case of assignment, which means that Article 165 CO would be applicable in principle. On the other

---

239 Pöschel/Maizar 2012: Art. 973*c* OR N 55 and other references; on the transfer of memberships, see also section 5.1.2.3 above.

240 See Girsberger/Hermann 2015: Art. 165 OR N 1; Gauch/Schluep/Emmenegger 2014: margin no. 3415 et seq.; von der Crone/Kessler/Angstmann 2018: 343.

241 Girsberger/Hermann 2015: Art. 165 OR N 1; Gauch/Schluep/Emmenegger 2014: margin no. 3415 et seq.; Spirig 1993: Art. 165 OR N 4.

242 See Art. 263 para. 3 CO und Art. 333 para. 1 CO.

243 Girsberger/Hermann 2015: Art. 164 OR N 4a.

244 Judgment of the Federal Supreme Court 4A_258/2014 of 8 July 2014, E. 1.3; Bucher 1988: 592-593; Bauer 2010: margin no. 206 et seq. and 231-232, and other references in each.

245 Bauer 2010: margin no. 236 et seq. and other references; Gauch/Schluep/Emmenegger 2014: margin no. 3548 and other references.

246 Judgment of the Court of Appeal of the Canton of Zurich LB100081-O/U of 20 December 2011, E. 4.3.1.

247 Blockchain Taskforce 2018b: 14.

hand, some scholars also argue that the transfer of a token can be interpreted as the implied conclusion of a tripartite agreement for assumption of the contract.[248] Such an agreement might *a maiore ad minus* also cover only individual claims. This classification is based on the view mentioned above that all tokens – regardless of the content attaching to them – are to be understood as a claim of recognition against any other participant in the system.[249] This view holds that, by entering the transaction into the system, the holder of a token applies to all participants in the system to transfer the holder's claim of recognition to the acquirer of the token. Since all the participants in the system have agreed to abide by the rules of the protocol, they – as obligors of the right to recognition – are collectively involved in the transfer. Provided that validation is in conformity with the protocol, it can then be said that they have given their consent to the transfer in advance. By storing the transaction on the blockchain in accordance with the rules of the protocol, a transfer agreement on the right to recognition would thereby be concluded between all the legal subjects involved, without any further requirement as to form. But as discussed above in the example of cryptocurrencies, it appears uncertain whether such an intention by the individual users of the blockchain to be legally bound, with the associated contractual consequences, can in fact be construed.[250] Already today, there are constellations in which not all users of a blockchain assume the same preconditions, for example by employing the "coloured coins" method on existing blockchains to transact individual contractual relationships whose content is known only to the users involved.[251] Where tokens are intended to represent a claim against an issuer, it furthermore appears uncertain whether the acceptance of such a large number of contracting parties corresponds to the expectations of the parties.

c) Conclusion

The written form is prescribed by law for the transfer of a claim, so that as a rule the signature in the hand of the assignor is required. The same applies to claims and other rights structured as uncertificated securities. Whether the transfer of a token alone can be used to transfer an entire associated contractual relationship has not yet been clarified conclusively by case law. Similarly, there is no established view in the relevant academic literature. The answer is likely to depend heavily on the circumstances of the individual case.

5.1.4.3 Property (including certificated securities)

a) Principle: Physical delivery (*traditio*)

Under the principle of causality prevailing in Swiss property law, the transfer of ownership requires a valid act creating a legal obligation (*causa*) and, as a rule, the transfer of possession of the object (*traditio*). By transferring possession, the transfer of ownership becomes visible to third parties, thus serving to uphold the principle of publicity.[252] Negotiable securities are in principle also transferred with the transfer of possession of the instrument, although further requirements may apply depending on the type of security.[253] Direct delivery of chattel is not the only way to obtain ownership, however. Several surrogates for physical delivery are available to transfer possession and thus ownership without direct delivery of an object in person.

248 von der Crone/Kessler/Angstmann 2018: 343 et seq.
249 See section 5.1.2.5 above on the legal classification of crypto means of payment.
250 See section 5.1.2.5
251 Meinel/Gayvoronskaya/Schnjakin 2018: section 3.2.1 (Colored Coins).
252 Rey 2007: margin no. 1720-1721.
253 Art. 967 para. 1 and 2 CO.

b) Providing the means to gain effective control of an object

First of all, possession can be transferred with the help of means by which the recipient may gain effective control of an object.[254] A classic application is the handing over of a car key. In the case of *smart property*, it is conceivable that the means for gaining effective control might also be effected by transferring a token.[255] This may apply if the object is stored in a safe that can be opened only with a token. In such cases, the transfer of a token is suitable for transferring ownership of a movable object if the transfer is based on a valid act creating a legal obligation.

c) Transfer of possession by means of a legal transaction (surrogates for physical delivery)

An object does not actually have to be delivered if it is in the custody of a third party which will continue to keep the object in custody.[256] This scenario is referred to as direct and indirect possession. The owner who has an object kept in custody by a third party remains the party with indirect possession of the object, while the third party exercises direct possession. If the object is to be sold but still held in custody by the third party, it is sufficient to transfer indirect possession by means of instructions to that effect.[257] The transferor and the acquirer enter into a possession transfer agreement which is not subject to any formal requirements and in that way transfer ownership. The transfer of ownership becomes effective vis-à-vis the party with direct possession when the transfer is notified to that party.[258] The instructions to transfer possession can be securitised, which is typically the case with documents of title to goods.[259] The custodian undertakes to exercise direct possession of the goods for the respective holder of the document of title to goods. The transfer of the indirect possession of the goods (and thus of ownership) can take place by physically delivering the document of title to goods; in such cases, notification to the party with direct possession of the goods is unnecessary.[260]

Transfer of ownership by means of a legal transaction is also possible if the transferor of an object retains direct possession of the object on the basis of a special legal relationship.[261] This is considered a case of constructive possession.[262]

According to the case law of the Federal Supreme Court, however, assignment of the claim to delivery under Article 641 para. 2 CC (*vindicatio*) does not constitute a permissible surrogate for physical delivery.[263] Assignment of the claim to vindication cannot be used to transfer ownership of an object.

It is conceivable that in all cases where the ownership of an object and direct possession do not coincide, the ownership relationships are represented in a decentralised register. If it is the clear intention of the parties to transfer ownership of an object held by a third party or a part thereof by transferring a token, the transfer of the token can be seen as the expression of an informally concluded agreement to transfer possession. The transfer of the token can at the same time play the role of notification to the party with direct possession; that party knows that possession of the token is now on behalf of the new owner and that the object may in principle only be delivered to that new owner. A transferor who, due to a special legal relationship, remains in direct possession of an object may transfer ownership of that object or part thereof

254 Art. 922 para. 1 CC.
255 Eggen 2017a: 12-13.
256 On the establishment of ownership by means of constructive possession, see also section 5.1.2.4.
257 Art. 924 para. 1 CC.
258 Art. 924 para. 2 CC.
259 Art. 1153 et seq. CO; on documents of title to goods, see also section 5.1.3.2 b).
260 See Oftinger/Bär 1981: Art. 902 ZGB N 21.
261 Art. 924 para. 1 CC.
262 On constructive possession, see also section 5.1.2.4.
263 BGE **132** III 155 E. 6.1.

by way of constructive possession without any formal requirements – and thus in principle also by moving a token.

d) Conclusion

In order to obtain rights in rem such as ownership of an object – which also includes certificated securities – a valid act creating a legal obligation is required, as well as – in general – the transfer of possession. In principle, ownership can therefore not be transferred by moving a token. However, there are a number of constellations in which this is already conceivable under current law. On the one hand, if the transfer of the token transfers actual sovereignty over the object, ownership of the object can be transferred in this way. Use cases in this regard might arise in the case of *smart property*. On the other hand, in constellations where ownership and direct possession do not coincide, transfer is possible by means of an informally concluded agreement to transfer possession or by way of constructive possession. The intention to transfer indirect possession can also be expressed by moving a token. If the blockchain is public or at least viewable by the party with direct possession of the object, the movement of the token can also serve as notice to the party with direct possession, who now knows that possession is on behalf of a new owner.

5.1.4.4 Intermediated securities

Intermediated securities may be transferred by instruction of the account holder to the custodian and subsequent crediting to the securities account of the acquirer.[264] No form is prescribed for the instruction. However, it is stipulated that the entry be performed by a custodian referred to in Article 4 FISA.[265] As explained above, this requirement of a central custodian is likely not easily reconciled with the blockchain as a decentralised register.[266] If the requirements of the Federal Intermediated Securities Act are not met, classification of tokens as intermediated securities can be ruled out, which means that transfer under the Federal Intermediated Securities Act without formal requirements is also not available.

5.1.4.5 Cryptocurrencies

As explained above, the prevailing Swiss doctrine correctly classifies tokens in the form of cryptocurrencies (e.g. Bitcoin, Ether) as intangible assets.[267] Since they cannot therefore be classified either as absolute or as relative rights, the transfer rules provided for those categories do not apply either.[268] In other words, the law does not provide specifications for the transfer of cryptocurrencies. Their transfer takes place without formal requirements by making the *de facto* power of disposal or access available. There accordingly appear to be no legal obstacles that would stand in the way of a transfer.

5.1.5 Conclusion

From the point of view of civil law, two types of token can be distinguished.

Firstly, there are tokens that primarily represent a value within the blockchain context, e.g. a cryptocurrency such as Bitcoin. The second category of tokens are those intended to map and represent a right existing outside the blockchain. In the first case, the token itself has a value; in the second case, the parties intend for the token to be linked with a value outside the blockchain, or to represent such a value or provide access to it.

---

264 Art. 24 para. 1 FISA.
265 See Eggen 2018: 564-565.
266 See section 5.1.3.4 and Blockchain Taskforce 2018b: 15.
267 See section 5.1.2.5 and the references in n. 133.
268 But for a different view, see Blockchain Taskforce 2018b: 13; Weber/Iacangelo 2018: margin no. 51, which require the acquisition of "possession" for the transfer of crypto means of payment.

These two categories under civil law are not contradictory, but rather form the basis of FINMA's distinction between payment, utility, and asset tokens. This categorisation, which is also supported by the Blockchain Taskforce, is decisive for the classification of tokens under financial market law.[269] From the perspective of civil law, while payment tokens and asset tokens can generally be assigned relatively clearly to one of these categories, utility tokens can frequently also be assumed to constitute claims. Even if a token is intended to provide access to a service, for example, it may still be regarded as the representation of a claim similar to a contract for work and services or an agency contract.

Payment tokens or *native tokens*, the value of which is limited to applications on the blockchain, are – according to what is likely the prevailing view – purely *de facto* intangible assets. They cannot be assigned to any of the main categories under civil law. Civil law therefore does not impose any requirements – and therefore no obstacles – for their transfer. With regard to the transfer of cryptocurrencies (e.g. Bitcoin, Ether), there is therefore no need to adjust civil law.

Tokens that are intended to represent rights and make them tradable should, according to the intention of the users, fulfil a function similar to that which securities have traditionally played and continue to play. The tokens are intended to be linked to rights and to simplify trading in these rights, just as rights are traditionally linked to paper instruments and in that way made tradable. Under current law, however, tokens can perform this function only to a limited extent. Classification of tokens as "electronic securities" *de lege lata*, as advocated in part by the academic literature, is associated with legal uncertainty. While tokens may be amenable to the contractual attachment of uncertificated rights, this does not facilitate the transfer of or trade in those rights. In light of their contractual nature, uncertificated securities alone cannot guarantee the functions of negotiable securities (proof of entitlement, transfer, protection of transactions); their transfer requires a written declaration by virtue of express statutory order. Whether the movement of tokens can be used to transfer entire contractual relationships without formal requirements has not been clarified conclusively and is likely to depend heavily on the circumstances of the individual case. Increased tradability is achieved if uncertificated securities are structured as intermediated securities. However, since the Federal Intermediated Securities Act assumes that the relevant postings are made by central, registered custodians, that law is also poorly suited to the decentralised world of blockchains.

To facilitate the trading of rights on the blockchain and to increase legal certainty, an *adjustment and further development of securities law* therefore appears to be called for. Since an entry in a decentralised register accessible to interested parties is able to create publicity similar to the possession of a certificated security, it seems justified to grant similar legal effects to such an entry. The established principles of securities law should be retained to the extent possible. Digital representation and transfer can therefore be considered only for those rights which could also be securitised in a negotiable security and which are amendable to unrestricted transferability. Such tokenisation is thus in principle ruled out for most rights in rem such as ownership of chattel and for most forms of membership under company law. In particular the digital representation and transfer of ownership of real objects existing in parallel would raise numerous legal questions – with the exception of constellations of tiered possession in which transfer of ownership by means of legal transactions is already possible under current law. It therefore appears conceivable that this transfer by means of a legal transaction may be expressed by moving a token – even under existing law. A need for action under civil law is not apparent in these constellations.

Legal amendments concerning the transferability of rights via tokens could – as one of the alternatives envisaged in the Blockchain Taskforce's position paper – start with uncertificated securities. Under current law, rights that can be securitised can also be structured as

[269] See section 6.2.

uncertificated securities. If these uncertificated securities are kept in the central register of a custodian in accordance with Article 4 FISA, they become intermediated securities and can be transferred by means of digital posting of transactions. Amendments to the law could achieve that postings in decentralised registers would also be able to effect the transfer of uncertificated securities. Uncertificated securities – the content of which is now limited to the basis for the creation of intermediated securities – would thus be upgraded to a new, fully-fledged category of securities law. At the detailed level, there are still many open questions that would have to be addressed when drafting the amendments to the law. The central question here is which requirements such a register entry would have to fulfil in order to justify the attachment of legal effects. The effects of this change under financial market law must also be taken into account, in particular the effects on securities trading. Finally, it must also be examined whether such a further development of securities law would open up new possibilities for abuse, which would in turn have to be addressed by legislation as well.

5.2 Treatment of crypto assets and data in insolvency proceedings

5.2.1 Statement of the problem

An important question to be answered with regard to crypto assets concerns their treatment in an insolvency proceeding. As stated, cryptocurrencies – regardless of their specific design and legal classification – are generally considered as assets; they can therefore be seized by the creditors of the person entitled to them. At least in the case of the more common cryptocurrencies (e.g. Bitcoin, Ether), subsequent realisation of the assets is also possible. And similarly in bankruptcy proceedings, in which the assets to which the bankrupt debtor is entitled are collected, realised, and distributed to the creditors in accordance with the legal requirements, realisation of the debtor's crypto assets is generally possible and therefore also called for.

In bankruptcy proceedings, it needs to be determined which values are to be included in the debtor's assets, in particular when assets of which the debtor is a beneficial owner are subject to the power of disposal of a third party, or when the debtor has control over assets to which third parties assert their own beneficial ownership.[270] In the present context, clarification of this question is particularly important in the case of third-party safekeeping of crypto assets by wallet providers, since in such legal relationships the beneficial ownership and the power of disposal over the assets may not coincide.

5.2.2 Segregation of crypto assets in bankruptcy – current law

5.2.2.1 General principles

In practice, crypto assets are often not held in custody by the beneficial owner but rather by a third party. This can be explained by the fact that such third party custody creates certain advantages for the beneficial owner in terms of functionality, thus providing access to functions that would otherwise not or not as easily be accessible without the intermediary. This is because the custodian can usually perform certain transactions more directly and easily, such as converting one cryptocurrency into another. The beneficial owner is also released from the task of administering numerous access keys: he needs only to have access to one account, while access to the individual tokens is administered by the custodian. But above all, custody by a professional third party regularly promises a higher level of security than custody by the owner, in particular with regard to a better protection against hacker attacks.

---

[270] Similar questions may in part also arise in regard to seizure.

If the wallet provider goes bankrupt, the question arises as to whether the crypto assets are included in the bankruptcy estate or whether they can be segregated, i.e. transferred to the beneficial owner (instead of the creditors in bankruptcy).[271] Because current law does not contain any special provisions with regard to the treatment of cryptocurrencies in the event of bankruptcy, the general provisions of the Debt Enforcement and Bankruptcy Act (DEBA)[272] as well as any special provisions under financial market law apply.

5.2.2.2 Inclusion in the bankruptcy estate

Whether an asset is part of the bankruptcy estate or not is primarily determined by who has custody of the asset (Art. 242 DEBA). For chattels that are in the debtor's possession, the DEBA establishes a presumption that the debtor is the beneficial owner. Anyone who claims to have a better right (in particular property rights) with regard to the object must pursue such a claim by segregation proceedings pursuant to Article 242 para. 2 DEBA. If, on the other hand, the chattels are not in the possession of the bankrupt person, Article 242 para. 3 DEBA must first be applied in order to include the object in the bankruptcy estate for the purpose of realisation in bankruptcy (inclusion proceedings).

According to the case law of the Federal Supreme Court, segregation of physical property is necessary only if the bankruptcy estate has *custody over the assets*.[273] The Federal Supreme Court bases its analysis on the "exclusive actual power of disposal."[274] Along these lines, Article 242 para. 3 DEBA already expressly provides in the case of co-custody that the asset in question is not included in the estate. If this exclusive actual power of disposal is lacking, the bankruptcy estate therefore has no custody, and at best the disputed property can be added to the estate as part of inclusion proceedings.

The Federal Supreme Court's criterion of exclusive actual power of disposal can be used straightforwardly to decide whether a specific crypto asset is to be considered as part of the estate or not, since actual power of disposal is not linked to the tangibility of the asset concerned. As of today, the Federal Council is not aware of any court judgments that have ruled on whether crypto assets can be segregated or not.

Depending on the form of the specific circumstances of custody, the following distinctions can be made:

– A first distinction is made depending on whether the client retains direct access to the crypto assets or not. If the access key is known exclusively to the client, then only the client can directly dispose of it and initiate a transaction to that effect on the blockchain, but not the wallet provider. This means there is no third-party custody. And even if both the client and the custodian have identical access keys and can thus both directly initiate a transaction on the blockchain, it must be assumed that the beneficial owner retains actual power of disposal and that there is accordingly no third-party custody.

– The parties may also often agree on a setup in which access to the crypto assets requires not only one key, but rather several keys. Such a multi-signature address may require all of the keys (e.g. a "2 out of 2 multi-signature") or only some of the keys (e.g. a "2 out of 3 multi-signature"). If the bankrupt is in possession of a key that forms part of a multi-signature address, it is to be determined whether the crypto assets are part of the estate or not. As discussed above, the criterion of exclusive actual power of

---

271 Both the following discussion on current law as well as the considerations *de lege ferenda* concern only bankruptcies subject to Swiss law. To the extent the bankruptcy proceedings are carried out abroad, the provisions applicable in the respective countries apply.

272 SR **281.1**

273 BGE **110** III 87, 90

274 BGE **110** III 87, 90 and other references.

disposal must properly be applied here as well, with the consequence that the crypto assets are not included in the estate if the power of disposal is shared. [275]

As a conclusion, it can be held that crypto assets to which the client has direct access are not included in the bankruptcy estate. The same applies if more than one key is required to dispose of the asset and the bankruptcy estate does not have sufficient keys to single-handedly dispose of the crypto asset. In such cases, the bankruptcy administration must act if it wishes to realise the asset as part of the bankruptcy. Only where clients have no access of their own and the bankrupt at the same time has all the keys to access the asset directly is the asset included in the bankruptcy estate and must at best be reclaimed by the client with a better right to the asset through legal action. These rules also apply to the distribution of the procedural roles in a third-party objection procedure pursuant to Articles 106–109 DEBA.

5.2.2.3 Segregation under Article 242 DEBA

If the bankrupt in fact has exclusive actual power of disposal over the assets, there is a legal presumption that the bankrupt is also the beneficial owner. The assets are therefore in principle included in the bankruptcy estate, and the next question to be answered is whether they can be segregated. The question of how to proceed when power of disposal and beneficial ownership of assets do not coincide in a bankruptcy is by no means new; fiduciary transfers of assets have existed for a long time, as have the resulting difficulties in the event of insolvency of the fiduciary. The DEBA therefore provides for a procedure in such cases to achieve the proper allocation of assets. Of central importance in this discussion is the legal *distinction between property and assets*. Just as someone may be the owner of an object without it being part of that person's assets (where economically it belongs to a third party), a person may also be entitled to a certain asset without having a property right with regard to it or without such a relationship being possible at all, namely to contractual rights, but also to pure assets which – like cryptocurrencies – are neither in rem nor contractual in nature. Particularly in the context of insolvency, it must therefore always be considered whether the relevant legal consequence is linked to classification as an asset (e.g. for the purposes of garnishability and realisability) or to its quality as an object subject to property (e.g. for the purposes of segregation).

In this regard, the DEBA assumes a fundamental distinction between rights in rem and contractual rights: to the extent that a third party is the owner of an object, that object is not included in the bankruptcy estate or the third party may reclaim the object and segregate it from the bankruptcy estate (Article 242 para. 1 and 2 DEBA). As a consequence of the legal position in rem, the object as a whole is due to the entitled owner, and no *pro rata* satisfaction or participation of the other creditors takes place. If, on the other hand, the bankrupt debtor has acquired ownership of an object, the third party may be entitled to a contractual claim for repayment.

The situation is different for contractual rights. In the event of bankruptcy, these rights are satisfied only *pro rata*, i.e. creditors merely receive the right to satisfy themselves jointly with the other creditors from the proceeds of the bankruptcy, taking into account the ranking of creditors under bankruptcy law, which regularly results in only partial, i.e. *pro rata*, satisfaction of the claims.

As discussed above, the prevailing opinion on the law currently in force in Switzerland assumes that ownership under civil law is not possible in the case of data and information due to their lack of physicality.[276] It does not matter in this regard whether the custodian received the asset by way of transfer from the beneficial owner or acquired it from a third party as the indirect

[275] Hauser-Spühler/Meisser 2018: 11; Maurenbrecher/Meier 2017: margin no. 26.
[276] See section 5.1.

representative of the beneficial owner. According to this view, segregation based on Article 242 DEBA would not be possible:[277] Because Article 242 DEBA refers expressly to "objects", its scope of application is, according to prevailing doctrine[278] and "*largely unchallenged, clear and consistent case law of the Federal Supreme Court*"[279] in principle limited to the segregation of physical objects based on ownership under civil law. Contractual claims, in contrast, confer a corresponding claim only in the cases provided for by law.[280] According to the view presented above, segregation of data based on Article 242 DEBA is not possible *de lege lata*.

However, in the context of the special characteristics of blockchain technology and the tokens based on that technology, it is argued in the recent literature that crypto assets can be segregated already under current law.[281] As justification, it is argued in particular that unlike data, crypto assets can be attributed unambiguously thanks to the blockchain and can be neither falsified nor multiplied. This means that – despite their lack of physicality – sovereignty can be exercised over them, which justifies the provision of quasi in rem protection for them. For that purpose, it is argued that Article 242 DEBA should be expanded teleologically and that its scope of application should be extended to include cryptocurrencies (in particular Bitcoin).

So far, neither the Federal Supreme Court nor – as far as can be seen – a lower judicial instance has had the opportunity to adjudicate the question of the segregability of crypto assets. Accordingly, there is currently considerable legal uncertainty in this regard.

A particular situation exists with regard to the law governing *agency contracts*: according to Article 401 para. 1 and 2 CO, the principal may, where the agent is bankrupt, demand segregation from the bankruptcy estate of "claims against third parties" and, according to Article 401 para. 3 CO, "chattels" of which the agent took ownership in the agent's own name but on the principal's behalf. Interpretation of this provision poses considerable difficulties in practice, however, and it is disputed whether it also includes objects received by the agent from the principal (and not only, as the wording suggests, acquired for the latter by indirect representation). According to the case law of the Federal Supreme Court, segregation of money is in any case not possible if it is not kept in custody separately, in particular if the money of several creditors is kept on the same account.[282] Furthermore, according to the same decision, segregation is ruled out if the agent can freely dispose of the money.[283] In any event, the legal precondition is crucial that these are "claims against third parties" or "chattels" in order for the segregation claim to apply.

5.2.2.4 Conclusion

The discussion makes it evident that it has not yet been clarified conclusively whether crypto assets can be segregated on the basis of Article 242 DEBA currently in force. There is a great need for legal certainty for the parties involved, not least of all because the answer to the question has far-reaching consequences.

The discussion on the segregability of crypto assets makes it evident that there is a real practical need for segregation and that it would be justified in terms of the subject matter to provide a conclusive legislative basis for segregation claims for crypto assets. The Federal

277 See generally Maurenbrecher/Meier 2017: margin no. 25.
278 See Russenberger 2010: Art. 242 SchKG N 10 and other references; see also the numerous references in BGE **128** III 388-389.
279 See Russenberger 2010: Art. 242 SchKG N 10 and other references to case law.
280 Schober/Avdyli-Luginbühl 2017: Art. 242 SchKG N 19.
281 Graham-Siegenthaler/Furrer 2014: margin no. 58 et seq.; Hauser-Spühler/Meisser 2018: 9 et seq.; Reiser 2018: 815 et seq.; Schönknecht 2016: 309 et seq.; Seiler/Seiler 2018: margin no. 71; Maurenbrecher/Meier 2017: margin no. 26; Meisser/Meisser/Kogens 2018: margin no. 45.
282 BGE **102** II 103
283 BGE **102** II 103

Council endorses this view; it recognises the need for action and the need for settlement of the legal uncertainty, and it is prepared to propose the necessary adjustments of the relevant legislation. However, it would be important to restrict the legislative design of such a segregation right to assets that can unambiguously be assigned to the trustor. This corresponds to the rule for ownership under current property law. In contrast, segregation claims should not be extended to those cases in which it is not possible to unambiguously assign the assets to a specific person, since this would exceed the analogy with physical objects; as a rule, segregation claims are not available in such cases, in which the creditor has rather to make do with the bankruptcy dividend.

Accordingly, it is of crucial importance from this perspective whether the assets under the sovereignty of the bankrupt can be assigned individually to the entitled party or whether the claim to surrender – analogously to property law – has been voided by "mixing"[284] and thus transformed into a contractual claim. In the case of physical objects, this is as a rule relatively easy to determine: if, for example, money is transferred in a fiduciary capacity to a third party, the ownership of the trustor is preserved as long as the transferred banknotes can still be individuated, for example by being kept in a marked envelope in a safe. But as soon as the trustee mixes them with other banknotes or deposits them on an account where the trustee's own money or money of third parties is also kept, the trustor's ownership is lost and the claim for surrender becomes a contractual claim.

These principles can also be applied to crypto assets: if the access key is no longer available to the client, a distinction must be made as to how crypto assets are allocated by the wallet provider. For instance, each client's credit balance may be assigned to a specific blockchain address and registered directly on the blockchain. This solution corresponds to a deposit in a safe deposit box or a securities account at a traditional bank. In this way, it is possible at any time and without additional technical arrangements[285] to assign the assets to the individual client for whom the custodian holds the cryptocurrencies. It is possible in this regard (as in the case of a securities account) that the credit balances have been acquired by the custodian for the client or that the client has acquired them elsewhere and subsequently transferred them to the custodian. If the credit balances of the custodian's clients are no longer assigned to individual blockchain addresses, then the clients only have a credit balance vis-à-vis the custodian. The custodian in turn should have the corresponding amount available in the cryptocurrency. It is mainly decisive in this regard that only the custodian has the access key. Such a solution corresponds to a traditional bank, which does not keep its client deposits separate, but rather has become the owner of the deposited money due to mixing. The credit balances of the client are then no longer visible on the blockchain, but rather can be deduced exclusively from the custodian's internal ledger.

5.2.3 Extension to all data

With the clarification of the statutory right of segregation for crypto assets, it would also be necessary to determine what constitutes the object of segregation (the crypto asset itself or only the access key). This question might be left open if, in addition to a claim for transfer of the crypto assets, an additional legal provision were introduced to provide for the segregation of data to which the beneficiary is able to demonstrate a special entitlement. This would simultaneously solve another problem that is generally recognised in practice and has recently been taken up by parliamentary initiative 17.410 Dobler ("Data are the greatest good of private

284 Art. 727 para. 1 CC.

285 In this case, the custodian must keep an account of which address or which access key is assigned to which client.

companies. Regulating the surrender of data in the event of bankruptcy of providers"). The initiative calls for Article 242 DEBA to be amended as follows:

> "The *bankruptcy administration shall issue an order on the surrender of non-physical assets which are claimed by a third party. As a precondition for surrender, the non-physical assets must be capable of segregation and the applicant must be able to substantiate that the assets are merely entrusted to the debtor. The costs incurred shall be borne by the applicant.*"

On 3 May 2018, the Legal Affairs Committee of the National Council unanimously endorsed the initiative, thus recognising the need for action. Examples cited in this context include company data that is stored in the cloud and can no longer be accessed in the event of bankruptcy of the provider, such as a client file or accounting data. But such situations may also arise in the private sphere, for instance if someone has uploaded private photos using a cloud service that subsequently files for bankruptcy. In all these cases, access to the data may no longer be available due to the bankruptcy if the bankruptcy administration no longer allows the servers to operate.

Under these circumstances, the Federal Council considers it appropriate – analogously to the segregation claim of the owner under property law – to create a suitable legal basis that would make it possible to segregate from the bankruptcy estate all data for which a person can prove special personal entitlement.

To avoid problems of demarcation, this surrender claim should not be limited to rights pertaining to assets, but rather should include all data. This would also cover items or rights that cannot be realised because they do not have an objective asset value. Legal positions of that kind are currently not subject to bankruptcy proceedings.[286]

5.2.4 Conclusion

The Federal Council recognises that there is a need for action with regard to both crypto assets and other digital data. As part of the planned consultation, the Federal Council will therefore propose a provision setting out a right to the surrender of data in the event of insolvency, including a claim to the transfer of crypto assets. Such an approach would solve the problems discussed and clarify the existing legal uncertainty without creating a new ownership position for data, which, in the view of the Federal Council, might have far-reaching and unforeseeable consequences.

5.3 Private International Law

5.3.1 Preliminary remarks

If the place of business, seat, domicile, or habitual residence of the issuer, seller, or recipient of a token is outside Switzerland, or if there is any other significant link to a foreign country, the question arises from a Swiss perspective to what extent the Swiss courts have jurisdiction over any dispute and which law they would have to apply. The principles set out in section 5.1 are valid only if Swiss law applies. If a foreign judgment has already been issued, the question must be answered of whether it can be recognised in Switzerland. The answer to all these questions is derived primarily from the Federal Act on Private International Law (PILA).[287] For questions of jurisdiction and recognition of foreign decisions, the Lugano Convention (LugC)[288] must also be observed; as a treaty, the Lugano Convention takes precedence over the PILA[289] and applies in principle where the defendant's domicile is in Switzerland or another state bound

---

286 Art. 197 para. 1 DEBA.
287 SR **291**
288 Convention of 30 October 2007 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, SR **0.275.12**.
289 Art. 1 para. 2 PILA.

by the Convention.[290] For certain sub-areas and in bilateral relations with individual states, other international treaties are of importance, but they will be dealt with only selectively here.

Where foreign courts have jurisdiction, the applicable law is determined by the relevant provisions of that foreign country.

The treatment under private international law of issues involving tokens depends on the intended function of the token in question. According to the discussion in section 5.1.2, four categories of values can be distinguished that may attached to a token:

1. Claims
2. Memberships
3. Rights in rem
4. Cryptocurrencies

The current legal situation is outlined below with regard to these four categories. The following discussion refers exclusively to disputes under private law (e.g. between the issuer or seller of a token and the recipient). The scope of Swiss financial market legislation and the responsibilities of the relevant authorities are governed by their own rules.

5.3.2 Jurisdiction of the Swiss courts

5.3.2.1 Contractual designation of the place of jurisdiction

The parties may in principle determine the place of jurisdiction themselves.[291] For instance, the issuer of a token may include a jurisdiction clause in its general terms and conditions. Disputes concerning rights to real estate are excluded.[292]

However, under the PILA, consumers[293] cannot waive the place of jurisdiction at their place of domicile or habitual residence in advance.[294] A similar rule applies under the Lugano Convention.[295] The place of jurisdiction at the place of issue referred to in section 5.3.2.5 may likewise not be excluded by an agreement conferring jurisdiction.[296]

Instead of a place of jurisdiction, the parties may also provide for the competence of an arbitral tribunal.[297]

5.3.2.2 Tokens linked to a claim

Under Articles 112 et seq. PILA, actions relating to a claim based on a contract are classified as "actions arising out of a contract".[298] Also under the Lugano Convention, these are considered contractual disputes. The jurisdictions set out in Articles 2, 5(1), and 5(2) of the Lugano Convention apply.

---

290 These countries include all EEA members with the exception of the Principality of Liechtenstein.
291 Art. 5 para. 1 PILA, Art. 23 LugC.
292 Art. 97 PILA, Art. 23 para. 5 in conjunction with Art. 22 para. 1 LugC.
293 See section 5.3.2.2 and section 5.3.2.6.
294 Art. 114 para. 2 PILA.
295 Art. 17 LugC, with a narrow exception in Art. 17 para. 3 LugC.
296 Art. 151 para. 3 PILA.
297 Art. 7 PILA. The case law of the Federal Supreme Court (see BGE **136** III 467 E. 4.2 et seq.) suggests that an arbitration agreement is permissible also in the areas mentioned above, in which an agreement conferring jurisdiction is excluded.
298 An exception applies to liability claims in connection with public issues. See section 5.3.2.5.

Depending on the circumstances, an action in Switzerland may be brought in the following places (provided they are located in Switzerland): the domicile/seat,[299] habitual residence[300] or the involved place of business of the defendant or at the place of performance of the contract. The place of performance is determined differently depending on whether the PILA or the Lugano Convention is controlling. The decision is in some constellations based on the performance that is characteristic of the contract and in other constellations on the performance constituting the subject matter of the legal dispute.

It is questionable, however, to what extent a place of performance can be located at all for contracts underlying a token, since the performance of the service in question often takes place on the internet.[301] In the case of utility tokens, for example, the performance characteristic of the contract is access to a service provided on the internet.

If the complainant qualifies as a consumer[302] and if the complainant's domicile or habitual residence is in Switzerland, the complainant has the option of filing the claim in the judicial district of that domicile or habitual residence.[303] The Lugano Convention provides for similar special treatment of consumer contracts.[304]

5.3.2.3 Tokens linked to membership

Actions concerning a membership right embodied in a token are classified as "disputes under company law" under Article 151 PILA. However, this provision has been largely superseded by the Lugano Convention. Once again, the jurisdiction rules set out in Articles 2, 5(1),[305] and 5(5) of the Lugano Convention apply.[306] The Lugano Convention provides for specific jurisdiction under company law only for disputes relating to the existence of the company.[307]

5.3.2.4 Tokens linked to a right in rem

If the token is intended to embody a co-ownership share or a claim secured by a pledge, Articles 97-98 PILA apply to disputes relating to the right in rem concerned. These provisions are again largely superseded by the Lugano Convention.[308] Under those provisions, actions may be brought in Switzerland primarily if the object is located in Switzerland or if the defendant is domiciled in Switzerland, depending on whether the object is immovable or movable.[309]

If the token corresponds to a document of title to goods,[310] the provisions mentioned above likewise apply to actions concerning ownership of the good in question.

---

299 A domestic place of jurisdiction exists even where a company only has the seat of its "central administration" or "principal place of business" in Switzerland (see Art. 60 para. 1 LugC).

300 If no domicile in Switzerland or other LugC member exists.

301 See Bonomi 2011: Art. 113 IPRG N 28.

302 See BGE **132** III 268 E. 2.2.3.

303 Art. 114 para. 1 PILA. It is disputed in the literature whether this alternative place of jurisdiction excludes those under Art. 112 para. 2 and Art. 113 PILA.

304 Art. 15 et seq. LugC. The concept of consumer contract should be interpreted more broadly than its counterpart in the PILA. Contracts with private investors are likely to be covered here in principle (see Judgment of the European Court of Justice of 28 January 2015 in Case C-375/13 *Kolassa*, margin no. 23-24).

305 This provision is also applied to disputes under company law (Hofmann/Kunz 2016: Art. 5 LugÜ N 77).

306 See section 5.3.2.2. In special cases, Art. 5(3) LugC may apply (see Hofmann/Kunz 2016: Art. 5 LugÜ N 479).

307 Art. 22(2) LugC. According to this provision, the seat of the company as defined in Art. 21 para. 2 PILA is decisive. Action may also be brought at this seat of the company if, in the case of an action within the meaning of Art. 151 para. 2 PILA, the domicile of the defendant is situated in a country not covered by the LugC.

308 Primarily Art. 2 para. 1 and 22(1) LugC.

309 Beyond the scope of the LugC, movable property is also subject to jurisdiction at the place where it is situated or at the habitual residence of the defendant.

310 While a document of title to goods does not embody a right in rem, it may serve to transfer such a right (see section 5.1.3.2.b).

If the dispute concerns the contract underlying the token issue, for instance a loan or transport agreement, the discussion in section 5.3.2.2 applies.[311]

5.3.2.5 Prospectus liability actions

In addition to the regular jurisdictions under company law in accordance with Article 151 para. 1 and 2 PILA,[312] elective jurisdictions are available at the Swiss place of issue, if any, for "actions arising out of liability as a result of the public issue of equity securities and bonds"; these actions are also referred to as "prospectus liability actions".[313] Prospectus liability actions are also conceivable where a token corresponds to an equity security[314] or bond.[315] Questions arise from the fact that tokens are issued on the internet, which makes it difficult to locate the place of issue.[316]

If, however, the defendant is domiciled in Switzerland or in another state bound by the Lugano Convention, the provisions of the latter apply. The Lugano Convention does not provide for a special place of jurisdiction for prospectus liability actions. However, according to the case law of the European Court of Justice on the Brussels I Regulation,[317] the general jurisdiction at the place of residence or the involved place of business of the defendant[318] is supplemented by an alternative place of jurisdiction in accordance with the rules applicable to torts.[319]

5.3.2.6 Reselling of a token

If a right associated with a token is resold and if the dispute revolves around the respective contract of sale, Articles 112-114 PILA or the provisions of the Lugano Convention governing contractual claims apply.[320] Here again, it may be difficult to locate the place of performance, given that the token is transferred over the internet.

If the dispute does not concern the contract of sale itself, but rather the entitlement to the right sold or to be sold, the jurisdictions referred to in sections 5.3.2.1 to 5.3.2.3 once again apply.

Where claims or memberships attached to a token have been credited to a securities account within the meaning of the Hague Securities Convention,[321] Article 108b PILA applies to disputes concerning the transfer or pledging thereof.[322] That article provides for the same jurisdictions as Article 112 PILA. Overall, a similar rule applies under the Lugano Convention,

---

311 The characteristic performance of a contract of transport is the transport in question (Art. 117 para. 3 let. c PILA).

312 See Eberhard/von Planta 2013: Art. 151 IPRG N 9.

313 Art. 151 para. 3 PILA. If the instrument is issued through the Swiss branch of a foreign company, the literature (see e.g. Vischer 2004: Art. 151 IPRG N 4) states that jurisdiction should also be assumed at that location. The primary regulatory subject matter of Art. 151 para. 3 PILA is that of prospectus liability actions. According to the Dispatch of 10 November 1982 on the Federal Act on Private International Law (PILA), however, the provision is also intended to establish non-derogable competence "with regard to the Swiss provisions for the protection of bondholders" (see BBl **1983** I 263, 293).

314 See section 5.3.2.3.

315 See section 5.3.2.2.

316 See the discussion on the place of performance in section 5.3.2.2 above.

317 See Judgment C-375/13 *Kolassa* referenced above, margin no. 36 et seq. The Federal Supreme Court has not yet ruled on the question, but its previous case law has in practice not deviated unnecessarily from that of the ECJ.

318 Art. 2 and 5(5) LugC.

319 Art. 5(3) LugC. According to standing case law, the complainant has two available places of jurisdiction, namely one at the place where the event giving rise to the harm occurred and one at the place where the harm arose.

320 See section 5.3.2.2.

321 Hague Convention of 5 July 2006 on the Law Applicable to Certain Rights in Respect of Securities held with an Intermediary, SR **0.221.556.1**

322 Art. 108a et seq. PILA should be understood in the sense of the broad definition of securities contained in the Hague Convention (Costantini 2012: Art. 108*a* IPRG N 7 et seq.).

where Articles 2 and 5(5) apply. The Lugano Convention does not contain specific provisions on securities in the custody of intermediaries.

5.3.2.7 Tokens as cryptocurrencies

As a rule, disputes relating to tokens of this kind are likely to concern a claim for payment. The question of jurisdiction must therefore be based on the contract on which the obligation in question is based. See section 5.3.2.2 in this regard.

5.3.3 Applicable law

5.3.3.1 Extensive choice of law

From a Swiss perspective, the law applicable to a token transaction can largely be determined by means of a choice of law. The issuer of a token linked to a claim may in principle specify the law applicable to the claim and its transfer in the terms and conditions of the token.[323] Such a choice of law is in principle binding on the Swiss courts. Moreover, if the token is resold, the parties to the contract of sale in question may designate the law applicable to that contract.[324] In both cases, this is subject to the exception for contracts with persons covered by the legal rules for consumers.[325] Moreover, there is no choice of law for prospectus liability actions.[326] Company law and property law matters are governed by the law applicable to the company concerned or the law at the place where the object in question is located respectively.[327] But there is also a limited choice of law available for the pledging of tokenised rights and the transfer of rights in rem.[328]

5.3.3.2 Tokens linked to a claim

Claims arising out of a contract are governed by the law applicable to that contract. In principle, the contracting parties may choose this law themselves.[329] Most likely, many issuers of tokens will set out the applicable law in their general terms and conditions.

Otherwise, Article 117 para. 1 and 2 PILA apply: "In the absence of a choice of law, the contract shall be governed by the law of the state with which it is most closely connected. [-] It is presumed that the closest connection exists with the state in which the party that is to provide the characteristic performance is habitually resident or, if that party has concluded the contract by virtue of professional or commercial activity, in which the place of business of the party is situated." In the case of utility tokens, the characteristic performance is provided by the contracting party that grants the utility in question, i.e. the party issuing the token.[330] This means that as a rule, the law at the seat of that party's place of business applies.[331] Depending on the doctrine, the law at the seat of the issuing company or the law at the place of issue is determinative in the case of bonds.[332] This rule must also apply to tokenised bonds. In this case, however, the link must probably be established with the seat of the issuer, given that the place of issue is difficult to determine for tokens issued on the internet.

---

323 See section 5.3.3.2.
324 See section 5.3.3.6
325 See section 5.3.3.2.
326 See section 5.3.3.5; but the complainant has a statutory choice of law.
327 See section 5.3.3.3 and section 5.3.3.4.
328 Art. 105 para. 1 PILA and Art. 104 PILA.
329 Art. 116 para. 1 PILA.
330 See section 5.3.2.2.
331 This law also applies if the user is granted an intellectual property right (Art. 122 para. 1 PILA). Here again, any choice of law takes precedence (Art. 122 para. 2 PILA).
332 See Bonomi 2011: Art. 117 IPRG N 35 and other references. Under Art. 1157 para. 1 CO, the provisions set out in the Code of Obligations governing communities of bond creditors (Art. 1157-1186 CO) determine their own territorial scope (at least according to Reutter/Steinmann 2012: Vor Art. 1157-1186 OR N 32 et seq.).

Where the person receiving the token qualifies as a consumer,[333] Article 120 para. 1 PILA sets out that the law of the state of habitual residence applies if the contract was concluded in one of the circumstances referred to in letters (a)-(c) of that provision. How this rule should be applied when contracts are concluded on the internet has not yet been fully clarified.[334] Choice of law is not possible within the scope of application of Article 120 PILA.[335]

It makes sense if the law applicable to the underlying contract is also applied to the question to what extent the embodiment of the claim in a token is legally valid and to what extent the transfer of that claim can be linked to the transfer of the token. This makes all the more sense given that the prevailing doctrine in securities law appears to rely on the same connecting factor.[336] However, the state of opinion in regard to negotiable securities is still heterogeneous. Accordingly, no clear statements can be made in regard to tokenised claims, either.

It might also be considered whether Article 106 para. 1 PILA, which governs the question of securitisation of claims in regard to documents of title to goods, should be applied analogously.[337] This approach is very similar to that of the approach described above, at least in terms of outcome: the law chosen by the parties of the underlying contract is decisive or, where no such choice has been made, the law at the seat of the branch of the issuer. While Article 106 para. 1 PILA requires that the chosen law be "designated in the token", this requirement is likely to be met in most cases. The issuer designates the law in the token terms and conditions defined by the issuer. To what extent the law referred to in Article 106 para. 1 PILA differs from the law applicable to the primary contract thus depends essentially on how the term "branch" used in Article 106 para. 1 PILA should be interpreted.

5.3.3.3 Tokens linked to membership

Membership rights are subject to the law applicable to the company in question. This is primarily the law under which the company has been constituted.[338]

The law applicable to the company also determines to what extent the embodiment of membership in a token is legally valid and to what extent the transfer thereof can be linked to the transfer of the token.[339]

5.3.3.4 Tokens linked to a right in rem

The content as well as the acquisition and loss of a right in rem are in principle governed by the law of the state in which the object in question is situated.[340] The applicable legal system also determines the extent to which the respective right in rem can be linked to a token. In the

---

333 See BGE **132** III 268 E. 2.2.3.

334 See Bonomi 2011: Art. 120 IPRG N 17 and other references.

335 Art. 120 para. 2 PILA.

336 See Zobl 2001: 109 and other references.

337 At closer glance, Art. 106 para. 1 PILA covers two questions: the question to what extent the instrument embodies the right to surrender of the goods, and the question to what extent the transfer of this right also entails the transfer of ownership of the goods. With regard to the first question, according to Girsberger/Gassmann 2018: Art. 145 IPRG N 15, the provision must be applied *mutatis mutandis* also to other securities embodying a claim. The doctrine based on literature from before the entry into force of the PILA (mentioned e.g. in Daeniker/Waller 2011, Art. 2 Bst. a-c BEHG N 18), according to which the question must be answered pursuant to the law of the place of issue, can now be considered obsolete.

338 Art. 154 para. 1 PILA.

339 See Girsberger/Gassmann 2018: Art. 145 IPRG N 15; Vischer/Weibel 2018, Art. 155 N IPRG 25 and Eberhard/von Planta 2013: Art. 155 IPRG N 13, as to the law applicable to analogous questions regarding negotiable securities.

340 Art. 99 et seq. PILA.

case of a movable object, the parties to a transaction have a limited choice of law.[341] Any such choice of law cannot be asserted against a third party, however.[342]

If the token corresponds to a document of title to goods,[343] Article 106 para. 1 and 3 IPRG are likely to apply. The legal systems designated by these provisions[344] thus determine to what extent ownership of the good is linked to the status of holding the token. In contrast, Article 106 para. 2 PILA does not apply, since a token cannot be classified as an object for purposes of the PILA either.[345] An analogous application of this provision to virtual objects does not appear to be called for.[346]

If the dispute concerns the contract underlying the token issue (loan agreement, transport agreement, etc.), the law applicable to that contract applies.[347]

5.3.3.5 Prospectus liability actions

Under Article 156 PILA, claims arising out of prospectus liability[348] in connection with the public issue of equity securities and bonds "may be asserted under the law applicable to the [issuing] company or under the law of the state in which the issue took place." Otherwise, the relevant provisions of the PILA on company and contract law[349] as well as the directly applicable provisions of Swiss civil law apply to equity securities and bonds.[350]

5.3.3.6 Reselling or pledging of a token

A dispute concerning the resale of a token is governed by the law applicable to the relevant contract of sale. In the absence of a choice of law, this is as a rule the law of the state in which the seller's habitual residence or involved place of business is located.[351] This again is subject to Article 120 PILA (consumer contracts).[352]

If the dispute does not concern the contract of sale itself, but rather the entitlement to the right sold or to be sold, the law governing this right again applies.[353] Article 145 PILA, which governs the assignment of a claim "by contract" does not apply in this case. A claim embodied in a token must be treated the same in this regard as a securitised claim[354] that is transferred not directly by contract, but by transfer of the instrument. It can nevertheless be noted that in the absence of a choice of law, Article 145 para. 1 PILA relies on the law applicable to the claim to be transferred.[355]

The traditional view is that the transfer of securities is governed by the law at the location of the instrument.[356] An analogous application of this principle to tokens does not appear to make

---

341 Art. 104 para. 1 PILA.
342 Art. 104 para. 2 PILA.
343 While a document of title to goods does not embody a right in rem, it may serve to transfer such a right (see section 5.1.3.2).
344 See the end of section 5.3.3.2.
345 See section 5.1.2.4.
346 See section 5.3.3.6.
347 See section 5.3.3.2.
348 On the material scope of Art. 156 PILA, see Watter/Roth Pellanda 2013: Art. 156 IPRG N 9-10.
349 See section 5.3.3.3 and section 5.3.3.2.
350 E.g. Art. 1156 CO (see also Reutter/Steinmann 2012: Art. 1156 OR N 15).
351 Art. 117 para. 3 PILA.
352 See section 5.3.3.2.
353 See section 5.3.3.2–5.3.3.4.
354 See Bonomi 2011: Art. 145 IPRG N 5. Art. 145 PILA is not applicable to the transfer of company shares or rights in rem (Bonomi 2011: Art. 145 IPRG N 4).
355 The fact that the parties to a token transaction cannot themselves determine the law applicable to that transaction seems reasonable in view of the securities-like nature of tokenised claims and the resulting public interest in the protection of transactions. At least a choice of law in this regard should not be assertable against third parties (see Art. 104 para. 2 PILA).
356 See Zobl 2001: 110; see Art. 106 para. 2 PILA.

much sense, given that there is no right to the token comparable to the right to the instrument[357] and, moreover, tokens can hardly be situated geographically. In addition, the link to the place of location can be problematic even in the case of securities, given that the location is variable, not always easily recognisable, and often due to chance.[358] It is also criticised that when several identical securities are transferred, different legal systems may apply.[359] To what extent a legally relevant transfer of the token has occurred must therefore be assessed according to the law from which the legal link of the token with the attached right arises. As discussed, this must be the legal system governing the right in question.[360] Ultimately, however, the question of law applicable to the transfer of tokenised rights cannot be deemed conclusively clarified, at least with regard to tokenised claims.[361]

The legal systems designated by Article 105 PILA are applicable to the pledging of a right attached to a token. Tokenised rights must be treated as negotiable securities for the purposes of this provision.[362] Not only claims are covered, but also company shares and in rem rights.[363] If the dispute concerns the contract underlying the pledge, the law applicable to the contract once again is controlling.[364]

Where claims or memberships attached to a token have been credited to a securities account within the meaning of the Hague Securities Convention, their transfer or pledging is assessed in accordance with the law designated by the Convention.[365] As a general rule, the Convention refers to the account agreement concluded between the financial intermediary and the account holder.

5.3.3.7 Tokens as cryptocurrencies

Also for the purposes of the PILA, cryptocurrencies cannot be considered currencies.[366] Article 147 PILA ("Currency") thus does not apply.

The means by which a debt can be settled is determined by the law applicable to the contract in question.[367] In the non-contractual law of obligations, cryptocurrencies are unlikely to play a role.

5.3.4 Recognition of foreign judgments

Foreign judgments in connection with tokens may under certain conditions be recognised in Switzerland.[368] One of these conditions is that Switzerland considers the state in question to be competent. This question is governed by the following provisions of the PILA:[369]

- for contractual disputes, Article 149 para. 1 and Article 149 para. 2 let. a, b, and d PILA;

---

357 See section 5.1.1.1.
358 See Girsberger/Gassmann 2018: Art. 145 IPRG N 15 and other references; Zobl 2001: 109, 111.
359 See Zobl 2001: 111-112.
360 See Zobl 2001: 111; Dasser 2016: Art. 145 IPRG N 4 and other references; Girsberger/Gassmann 2018: Art. 145 IPRG N 15, and Bonomi 2011: Art. 145 IPRG N 5 (concerning the transfer of company shares). Dasser 2016: Art. 145 N 6a and Girsberger/Gassmann 2018: Art. 145 IPRG N 15 argue that the connecting factor for the transfer of claims in the form of securities should be the registered office of the issuer. But the PILA does not provide any basis for that argument. As an alternative to the law applicable to the claim, the law referred to in Art. 106 para. 1 PILA is the more likely candidate (see section 5.3.3.2).
361 See section 5.3.3.2.
362 See Zobl 2001: 111 concerning uncertificated securities. The token itself cannot be pledged (see section 5.1.1.1).
363 See Müller-Chen 2018: Art. 105 IPRG N 5.
364 See above and section5.3.3.2.
365 Art. 108*c* PILA. Art. 108*a* et seq. PILA should be understood in the sense of the broad definition of securities contained in the Hague Convention (Costantini 2012: Art. 108*a* IPRG N 7 et seq.).
366 See section5.1.2.5.
367 See section5.3.3.2.
368 Governed by Art. 25 et seq. PILA.
369 On the classification of individual disputes, see section 5.3.2.

- for disputes under company law or disputes concerning prospectus liability, Article 165 para. 1 and 2 PILA;
- for disputes concerning rights in rem, Article 108 para. 1 and 2 PILA; and
- for disputes concerning the transfer or pledging of securities held in custody by an intermediary, Article 108d PILA.

Within the framework of the Lugano Convention, the jurisdictions referred to in section 5.3.2 above are also decisive for the question of recognition. As a general rule, judgments from states bound by the Lugano Convention must be recognised.[370] In the cases of interest here, the jurisdiction of the court of the state of origin may as a rule not be reviewed, unless the judgment was given in breach of the rules on jurisdiction over consumer contracts.[371] [372] The recognition rules of the Lugano Convention supersede those of the PILA as far as judgments from Lugano Convention states are concerned.[373]

5.3.5 Conclusion

The legal issues arising under private international law in connection with the issue or reselling of tokens can largely be satisfactorily subsumed under the existing provisions of the PILA. Significant legal uncertainty exists solely with regard to the question of the law applicable to the transfer of tokenised claims. Legislative clarification in the form of a supplementary provision in the PILA appears called for in this regard. This opportunity could also be used to fill the regulatory gap in regard to negotiable securities.

While problems also arise with respect to the localisation of certain links such as the place of performance of a contract or the place of issue of equity securities or bonds, this is a general consequence of digitalisation that is not specific to blockchains. The answer to these questions should be left to the courts. This is even more important in light of the courts' ability to take European case law into account as well.

In the area of court jurisdiction and the recognition of foreign judgments, many rules are already laid down by the Lugano Convention. Switzerland can exert only very limited influence on these rules.

5.4 Other legal questions

5.4.1 Data protection aspects of the blockchain

The relationship between blockchain and data protection has only rarely been the subject of legal research so far.[374] However, both theory and practice have largely accepted that, despite the use of cryptographic methods, it is possible to infer data about individuals.[375] Insofar as blockchains contain personal data, they must comply with data protection requirements.

What is decisive in regard to compatibility with data protection requirements is the specific design of a blockchain system. While the implementation of these requirements appears to be less problematic in the case of permissioned blockchain systems,[376] the basic characteristics of permissionless systems raise questions concerning compatibility with data protection. For

370 Art. 33 para. 1 LugC.
371 Art. 15 et seq. LugC.
372 See Art. 35 para. 1 and 3 LugC.
373 Markus 2014: margin no. 1446.
374 In addition to a series of legal contributions, the first recommendations of the French data protection authority *Commission Nationale Informatique & Libertés* (CNIL) of September 2018 for responsible data processors include a consideration of the use of blockchains from the perspective of data protection, see CNIL 2018.
375 Erbguth 2018: margin no. 18; Gervais 2018: 129; Isler 2017: margin no. 4, margin no. 24, margin no. 26; Stengel/Aus der Au 2018: 445.
376 See Isler 2017: margin no. 13; Stengel/Aus der Au 2018: 441.

instance, it is still unclear whether a (central) authority exists – despite the decentralised structure of blockchain systems – that might assume responsibility for purposes of data protection law.[377] From the perspective of the principle of data minimisation, the immutability of the blockchain ensured by technical means and the irrefutable presumption of the correctness of the data is problematic.[378] In this connection as well as due to the decentralised structure of blockchains, the academic literature often argues that certain legal claims (right of rectification, withdrawal of consent, deletion) cannot be enforced on technical grounds or only to a limited extent.[379] It is furthermore questionable whether the data transparency enshrined in the system, which allows all participants to view all transactions at any time – albeit in (partially) encrypted form – is compatible with the protection of privacy.[380] Finally, specific deficits can be identified in specific applications based on blockchains. For example, *smart contracts*, which continuously execute automated legal consequences on the basis of pre-programmed individual decisions, do not appear to be compatible with the envisaged right to verify automated individual decisions by a natural person.[381]

As an approach to solving these deficits from the perspective of data protection law, reference is sometimes made to the self-responsibility of the persons who feed their own personal data into blockchain systems[382] as well as the consent of the parties concerned as a justification for a breach of privacy.[383] [384] But at present the view appears to be prevailing that the storage of personal data in compliance with data protection is not in principle ruled out even on open blockchain systems. This compliance can for instance be ensured through appropriate technical measures and default settings that are amenable to data protection (*privacy by design and by default*),[385] the use of special blockchain technologies (e.g. the model of a *self-sovereign identity*),[386] or other measures (off-chain data storage, zero knowledge protocol).[387] At the same time, the potential of blockchain for data protection is being recognised. Provided that the technical design is appropriate, blockchains could for instance provide technical support for the control of personal data, transparency, and compliance with the purpose limitation.[388]

A detailed examination is therefore necessary to determine whether and by which measures a design of blockchain systems in compliance with data protection is possible. In its report, the French *Commission Nationale de l'Informatique et des Libertés (CNIL)*, which has already formulated initial recommendations for the use of blockchain systems in compliance with data protection, calls on the EU to formulate solutions at the European level.[389]

---

377 Different views are represented in the literature in this regard, see Stengel/Aus der Au 2018: 446-447. But the CNIL is of the opinion that every person is responsible for the purposes of data protection law who decides on the entry of data on a blockchain, see CNIL 2018: 2.

378 Isler 2017: margin no. 1; see CNIL 2018: 7; Wiatrowski 2018: margin no. 15, refers in this respect to the "right to be forgotten" set out in Art. 17 GDPR. For a qualification in view of the incompatibility with the principle of data mining, see Stengel/Aus der Au 2018: 441, 447.

379 Isler 2017: margin no. 39; Stengel/Aus der Au 2018: 448.

380 Isler 2017: margin no. 1.

381 Isler 2017: margin no. 41 et seq.; Stengel/Aus der Au 2018: 448; see Art. 19 D-FADP (BBl **2017** 7193, 7215).

382 Art. 12 para. 3 FADP and Art. 26 para. 3 D-FADP (Draft of the Federal Act on Total Revision of the Federal Act on Data Protection and amendment of other enactments on data protection, BBl **2017** 7193, 7219).

383 Art. 13 para. 1 FADP and Art. 27 para. 1 D-FADP; BBl **2017** 7193, 7219.

384 See e.g. Stengel/Aus der Au 2018: 449-450.

385 Erbguth 2018: margin no. 2 et seq.; Isler 2017: margin no. 35, 37; Stengel/Aus der Au 2018: 448; CNIL 2018, 8 et seq. For a different view in regard to open blockchain systems, see Gervais 2018: 130.

386 See Zanol/Czadilek/Lebloch 2018.

387 Stengel/Aus der Au 2018: 451-452.

388 See e.g. Isler 2018: margin no. 48; see Wiatrowski 2018: margin no. 31 et seq. and Stengel/Aus der Au 2018: 447.

389 See CNIL 2018 and other references on the CNIL website, www.cnil.fr > Technologies > Blockchain (as at 3 October 2018).

5.4.2 Registers on the blockchain

There are a great many registers with legal implications that are maintained by public authorities. Examples include the land register,[390] the commercial register,[391] but also the already mentioned examples for the pledge of livestock,[392] ships,[393] and aircraft[394] as well as for the reservation of ownership.[395] The debt enforcement register[396] is another example in this context. Each of these registers has its own legal basis, and usually associated ordinances and directives are in place to regulate the operation of the registers and their effects in more detail. Theoretically, it would be conceivable to maintain such registers with the help of blockchain technology.[397] This would require a change of system and a large number of legislative changes. However, given the fact that the public registers in Switzerland function perfectly and blockchain technology is still in rapid development, there is currently no need for action at the federal level.

5.4.3 Smart Contracts

A smart contract is a computer protocol, usually based on a decentralised blockchain system, which allows automated contract execution between two or more parties with previously coded data.[398] According to the concept's inventor, the simplest form of a smart contract is the vending machine, which releases the goods as soon as the price has been paid.[399]

Contrary to what its name suggests, a smart contract, as the doctrine largely agrees, is not a contract in the sense of the Swiss Code of Obligations, but rather a computer "technology" for contract execution.[400] The inventor himself defined it as a "computerized transaction protocol that executes the terms of a contract".[401]

A smart contract has various characteristics that could influence its qualification and legal effects, which is why they are briefly mentioned below. Firstly, no human intervention is required. The terms of the contract are first determined by the parties and then converted into machine-readable form so that performance and all other conditions are programmed and automatically verified by the system (computer routine).[402] In a sports bet with two parties, for example, the amount wagered is automatically transferred in electronic money from the loser to the winner as soon as the result of the game has been autonomously retrieved by the system on sports information websites.[403] Neither party needs to intervene in order for the contract to be executed. The second characteristic of a smart contract is that it is immutable, i.e. the code cannot be changed by any party.[404] It is thus the absolute embodiment of the principle *pacta sunt servenda*, which is incorporated into our legal system with a few exceptions (including *clausula rebus sic stantibus*, fraud, termination of open-ended contracts for good cause without

---

390 Art. 942 et seq. CC.
391 Art. 927 et seq. CO.
392 Art. 885 CC.
393 Federal Act on the Shipping Register; SR **747.11**
394 Federal Act on the Aircraft Register; SR **748.217.1**
395 Art. 715 CC.
396 Art. 8 DEBA.
397 Practical attempts have been made e.g. in the Canton of Geneva (Commercial Register; see https://www.ge.ch/demander-extrait-certifie-conforme-au-registre-du-commerce/verifier-extrait-numerique).
398 Definition in connection with the relatively uniform theory, see inter alia Bacon/Bazinas 2017: 2; Kaulartz/Heckemann 2016: 618; Meyer/Schuppli 2017: 204 et seq., 207; Weber 2018: 291-292.
399 Szabo 1997: 1.
400 Furrer 2018: 103 et seq., 109; Jaccard 2017: paras. 8-9; Meyer/Schuppli, 2017: 204 et seq., 208; Weber 2017: para. 2. On controversies: Trüeb 2018: 725.
401 Szabo 1996: 1.
402 Essebier/Wyss 2017: para. 35; Meyer/Schuppli 2017: 204 et seq., 209; Weber 2018: 291, 292.
403 Example from Trüeb 2018: 726.
404 Essebier/Wyss 2017: para. 35.

notice, etc.).[405] Thirdly, the smart contract is limited to the digital world. Typically, only electronic goods/services (exchange of digital goods, transfer of money, etc.) can be the subject of a smart contract.[406] In addition, the programmed conditions for contract execution must be verifiable digitally (true/false), which can be problematic with regard to legally vague terms.[407]

The application of classical private law to smart contracts raises questions due to the automated and immutable nature of contract execution technology. First of all, the exchange of mutual expressions of intent does not take place in the conventional way. Each party expresses an intent and the system serves as an intermediary. WEBER refers to this as a "matching system".[408] Therefore, although the computer system plays an important role in the contract formation process, it is not a contracting party. According to prevailing doctrine, a party cannot conclude a contract solely with the computer system, as this does not have a legal personality within the meaning of the Civil Code.[409]

The application of the current provisions on contract execution to a smart contract raises questions too, as it directly concerns that area.[410] In the event of poor contract execution, therefore, the question of liability arises, e.g. liability for programming errors or machine errors despite correct programming.[411] There is also the question of whether it is possible to apply Articles 197 and 367 of the Swiss Code of Obligations in certain cases of technical program defects.[412] Finally, the party anonymity inherent in blockchain technology is one of the biggest obstacles for the implementation of the existing contractual provisions.[413] If contracting parties wish to assert their rights, they inevitably have to know their counterparty.

As things currently stand, doctrine recommends that parties wishing to conclude a smart contract should provide for suitable mechanisms for possibly changing circumstances and dispute resolution.[414] There will certainly be further developments in the area of smart contracts, but as it is still in the embryonic stage, it seems premature to legislate at the moment.

405 Meyer/Schluppi 2017: 204 et seq., 217; Weber 2017: para. 18.
406 Kaulartz/Heckmann 2016: 618 et seq., 619-620.
407 Kaulartz/Heckmann 2016: 618 et seq., 620; Weber 2018: 291, 292.
408 Weber 2018: 291, 294.
409 Furrer 2018: 103, 107, 109; Glarner/Meyer 2017: margin 31; Weber 2018: 291, 294. Contra Beck 2017: 186.
410 See Weber 2017: para. 19; Weber 2018: 291, 296.
411 See Essebier/Wyss 2017: para. 41; Weber 2017: para. 25 et seq.
412 Weber 2017: para. 29.
413 Kaulartz/Heckmann 2016: 618 et seq., 620.
414 See only Weber 2017: para. 33 et seq.

6 Financial market law

6.1 Introduction

6.1.1 Overview

The various currently known and potential future uses of blockchain and distributed ledger technologies relate to Swiss financial market law in many different ways. This chapter examines issues in the individual laws and in the subject areas of Swiss financial market law, as well as showing possible courses of action and any need for change.

It looks into the classification of tokens under financial market law[415], aspects of the Swiss Federal Law on Banks and Savings Banks [416], Financial Market Infrastructure Act[417], Financial Institutions Act[418], Financial Services Act[419], the Collective Investment Schemes Act[420] and insurance law[421].

6.1.2 The role of FINMA's fintech desk

The Swiss Financial Market Supervisory Authority FINMA considers it important to be able to take into account appropriately and rapidly the changed circumstances arising from the impact of fintech and in particular from blockchain-based business models on the market. Hence it set up the fintech desk at end-2015, which bundles all enquiries relating to fintech. The aim of the fintech desk is to provide rapidly fintech-specific information to interested persons from the public, start-up companies and established financial service providers on questions of interpretation relating to financial market law. To this end, it set up its own contact channels (fintech website[422], fintech mailbox and fintech hotline).

Since the fintech desk started operations, a marked increase in enquiries has been observed. Whereas the fintech desk answered 270 enquiries relating to fintech in 2016, this rose to 453 in 2017. Interest in the blockchain area is especially large: around 100 enquiries were made in 2017 about ICOs in particular. A total of around 60 percent of fintech enquiries in 2017 were related to blockchain.

In September 2017, FINMA published guidelines[423] in which it indicated the points of contact between ICOs and applicable financial market law. In February 2018, FINMA published guidelines on the handling of enquiries from ICO organisers.[424] The guidelines set out the specific information that FINMA needs to process such enquiries from market participants. At the same time, they indicate which principles FINMA uses to analyse and reply to corresponding enquiries (see also the classification of tokens under financial market law in section 6.2). The principles in the guidelines were explained to groups of interested parties at several roundtables. Since the publication of the guidelines (in addition to enquiries on the subject handled free of charge), FINMA has received 130 formal requests[425] relating to the

---

415 See section 6.2.
416 BankA, SR **952.0**; see section 6.3.
417 FMIA, SR **958.1**; see section 6.4.
418 FinIA, SR [**954.1**], adopted by the Federal Assembly on 15 June 2018, entry into force planned for start of 2020; see section 6.5.
419 FinSA, SR [**950.1**], adopted by the Federal Assembly on 15 June 2018, entry into force planned for start of 2020; see section 6.6.
420 CISA, SR **951**.31; see section 6.7.
421 See section 6.8.
422 See www.finma.ch > Authorisation > Fintech (as at 14.11.2018).
423 See FINMA 2017.
424 See FINMA 2018a.
425 As at 3 December 2018.

assessment of concrete ICO models under financial market law. These requests are answered by FINMA's fintech specialists.

6.2 Classification of tokens pursuant to financial market law

6.2.1 Introduction

In its guidelines of February 2018[426], FINMA classified tokens issued in ICOs as asset, utility and payment tokens under financial market law. The classification set out by FINMA in its guidelines is, in the opinion of the Federal Council, a suitable guide to deciding the implications of financial market law for tokens linked to a business model and is also attracting interest internationally. The section below describes the three token categories from an economic point of view and outlines the regulatory implications.[427]

6.2.2 Asset tokens

From an economic point of view, asset tokens present a predominantly investment-related or speculative aspect (for the buyer). Unlike pure payment tokens, they represent real economic assets "outside" the blockchain. In particular, an asset token may consist of a claim against the issuer under contract law or a membership right according to corporate law. For example, some asset tokens promise a share of future company earnings or future capital flows. Depending on its economic function, a token can thus represent a share, a bond or a derivative financial instrument. The category of asset tokens can also include tokens that allow for the trading of standardised claims for the delivery of physical objects on the blockchain, especially if such claims are normally traded in the capital markets (e.g. trade in commodities).

The classification of asset tokens cannot be based solely on the tokens as a source of information, but must take into account the issuing conditions and the legal positions related to the token.

If a token is classified as a security in accordance with FMIA, this can have numerous regulatory implications. In this respect, the provisions of FMIA and FinSA are particularly relevant.[428]

6.2.3 Utility tokens

Utility tokens give access to a digital application or service provided on or via a blockchain-based infrastructure. Depending on their form, they are comparable to vouchers, chips or keys that can be redeemed for contractually owed services.

Like asset tokens, utility tokens are based on a contractual relationship (in the form of a claim). Utility tokens are generally uncertificated securities, as the related rights (such as the right to access a service) are fungible, and the duty to keep an uncertificated securities record applies.[429]

Unlike asset tokens, utility tokens cannot be considered as securities. The term "securities" within the meaning of FMIA only includes the requirement of suitability for mass trading and does not specify any content limits. Based on the purpose of FMIA[430], however, a relationship to the capital market is necessary. Thus, standardised claims geared towards real fulfilment outside the capital market do not come under the scope of FMIA. This means that concert

---

426 See FINMA 2018a.
427 For the classification of tokens under civil law, see section 5.1.
428 Regarding FMIA, see section 6.4; regarding FinSA, see section 6.6.
429 See section 5.1.3.3.
430 Within the meaning of Art. 1 para. 2 FMIA, the purpose of FMIA is to ensure the proper functioning and transparency of the securities and derivatives markets, the stability of the financial system, the protection of financial market participants and equal treatment of investors.

tickets or store vouchers, for example, are not subject to FMIA, although they may take the form of securities that may be suitable for mass trading.

However, if a token is issued to collect funds to start or develop a company or a platform that will not provide services until a later date, it is not a utility token at the time of issue, but an asset token. From an economic point of view, the focus for the issuer is on borrowing and for the buyer on the investment or speculation opportunity. There is thus a relationship to the capital market, and FMIA is applicable.

Utility tokens are not securities. Accordingly, secondary trading of utility tokens is not subject to either FMIA or SESTA.

As utility tokens may be used as a means of payment, the issue of such tokens is essentially subject to AMLA (see the comments below on payment tokens). Anti-money laundering regulation is not applicable in individual cases if the main reason for issuing the tokens is to provide access rights to the blockchain for non-financial applications.[431]

6.2.4 Payment tokens

Payment tokens are tokens which are actually accepted or intended by the ICO organiser to be accepted as a means of payment for acquiring goods or services or as a means of money or value transfer. This includes "cryptocurrencies" in the strict sense of the term, such as Bitcoin, and numerous cryptocurrencies resulting from forks or variations of Bitcoin, such as Bitcoin Cash, Bitcoin Gold and Litecoin. These were not issued in the form of an ICO, but the creation of cryptocurrencies by means of ICOs is feasible. Utility and asset tokens can also have the function of means of payment, as "hybrid" tokens. Unlike asset or utility tokens, traditional payment tokens constitute neither a contractual nor a material legal position. Instead they can be classified as *de facto sui generis* assets.[432]

As well as cryptocurrencies in the strict sense of the term, other tokens may also be designed and used as means of payment. Typical examples are tokens that, according to the ICO organiser, are "secured" with assets such as gold or state currencies and are primarily intended for the transfer of money or value.

From a regulatory point of view, the anti-money laundering provisions set out in section 7 are particularly relevant for payment tokens.

6.2.5 Conclusion

As indicated in the introduction, the Federal Council's approach assumes that the currently valid legal provisions also apply for tokens. Hence, any decision about the applicability of individual legal provisions to individual tokens must be based on the functional form of the individual token. Classification can make such decisions easier in some cases, but not replace them.

6.3 Banking Act (BankA)

6.3.1 Introduction

The professional acceptance of deposits from the public is subject to the Federal Law on Banks and Savings Banks (Banking Act, BankA[433]) and requires in all cases an authorisation from FINMA. Various fintech business models involve such acceptance of third-party money subject

431 "Accessoriness"; see Art. 2 para. 2 let. a no. 3 AMLO, FINMA Circ. 2011/1: margin no. 13 et seq.
432 See section 5.1.
433 SR **952.0**

to authorisation. This applies in particular to certain blockchain and DLT-based business models, which come under the scope of BankA and may require bank authorisation.[434]

The bank authorisation is geared to specific business models that may entail a high risk potential from the point of view of protecting clients and maintaining stability. The typical banking business involves a time limit transformation, with short-term deposits being accepted (deposit business) and this money being partially or fully used to grant long term loans (lending business). Banking regulation aims to minimise the risks inherent in banking business, such as liquidity and interest rate risks.

Fintech business models may come under the scope of banking regulation today, even if they do not operate a traditional banking business.[435] In this context, however, the Federal Council has already previously stated that the high requirements of BankA seem disproportionately strict for such (fintech) business models.[436] In banking law, there are therefore two interrelated key questions regarding blockchain- and DLT-based business models:

One topic concerns the applicability of BankA to the blockchain- or DLT-based business models and hence also the applicability of the authorisation requirement to such business models, given that many blockchain- and DLT-based business models do not operate the time limit transformation typical of banks. Various issues have already been addressed with the additions to BankA in 2017. It is worthy drawing attention to the newly created authorisation category (fintech authorisation), which enters into force at the start of 2019, as well as to the fintech innovation area (*sandbox*) and to the extension of the exemption for settlement accounts.

Another topic deals with the treatment of crypto-based assets if an institution subject to bank insolvency law becomes insolvent. It is still to be decided how creditors are protected in case of insolvency if they have entrusted their crypto-based assets to a bank for safekeeping. There is a need to clarify this issue, not least in view of the considerations on the general treatment of tokens in the event of insolvency in accordance with DEBA.[437]

6.3.2 Bank authorisation requirement and exemptions relevant for blockchain business models

6.3.2.1 Bank authorisation requirement

The professional acceptance of deposits from the public needs authorisation from FINMA and is subject to prudential supervision. In accordance with the provisions of banking law, the only parties authorised for the professional acceptance of public deposits are banks and, from January 2019, the persons indicated in Article 1b BankA[438] in the context of the fintech authorisation. Any party that permanently accepts more than 20 public deposits or that publicly offers to accept deposits is considered to be acting professionally.[439] All liabilities[440] towards

434 See FDF Explanatory report Fintech 2017b: 11. See in general Reiser 2018: 811 et seq.
435 See Reiser 2018: 822.
436 See FDF Explanatory report Fintech 2017b: 11. By contrast, Bärtschi/Meisser 2015: 113 et seq., 131 et seq. are critical regarding the benefit of applying BankA to custodians of virtual currencies and consider FINMA supervision of custodians of virtual currency units to be unsuitable for ensuring the protection of creditors and investors.
437 See section 5.2.
438 "Fintech authorisation". See the changes in BankA in view of FinIA (in force from 1 January 2019).
439 Art. 6 BankO
440 The term "public deposit" is broadly defined and set out in BankA. Additionally, FINMA has published a circular forbidding the acceptance of public deposits (see FINMA Circ. 2008/3). At the same time, the term "deposit" needs to be clarified; see in particular Schönknecht 2016: 300 et seq.

clients are deemed to be public deposits.[441] In accordance with rulings by the Federal Supreme Court, the central element of the concept of deposit is the obligation to repay it.[442]

Many fintech business models are based on the acceptance of third-party monies. Accordingly, blockchain- and DLT-based business models may come under the scope of banking regulations, e.g. the provision of account-like services that enable clients to hold tokens, provided that the service provider is obliged to make repayment. Such services are supplied, for example, by providers that offer safekeeping of tokens or more extensive services based on token safekeeping.[443]

The FDF established previously that the acceptance of Bitcoins may constitute a public deposit.[444] Legal studies also state that "virtual currencies" as private means of payment may come under the term "deposit".[445] The key features of the acceptance[446] of public deposits, as illustrated by Bitcoins, generally also apply for other functionally comparable tokens and are as follows: (i) the client cannot dispose of Bitcoins any time without the involvement of a dealer or custodian, (ii) the dealer or custodian has a repayment obligation to the client, and (iii) the accepted Bitcoins would be included in the bankruptcy assets of the dealer or custodian in the event of bankruptcy. Accordingly, the safekeeping of tokens is not considered to be a deposit business subject to authorisation in line with FINMA practice if the balance is transferred solely for secure safekeeping, is held (directly) on the blockchain and can be attributed to the individual client at any time.[447]

6.3.2.2 Exceptions (no bank authorisation needed)

In the BankA, the legislator defined the issuance of bonds as an exception to the professional acceptance of public deposits (see below).[448] Incidentally, the legislator transferred the task of clarifying the term "public deposit" to the Federal Council. The Federal Council can make exceptions if depositor protection is guaranteed.[449] Based on this authority, the BankO contains various exemptions[450] from the term of (public) deposit and the "professional" requirement and specifies which activities require bank authorisation. In connection with blockchain- and DLT-based business models, the following exemptions apply in particular:

Consideration for the acquisition of property or the use of services

The acceptance of money that represents the contractual consideration for the acquisition of property or the use of services is not deemed to be a deposit.[451] In such cases, the term "money" is functional. Accordingly, the same applies for tokens that are functionally comparable to money. The acceptance of tokens as a contractual consideration, such as the consideration in a contract of sale or exchange or payment for a service is thus not an activity that requires authorisation pursuant to the BankA.

---

441 Art. 5 BankO
442 See e.g. BGE **132** II 382, E. 6.3.1; BGE **136** II 43, E. 4.2; Federal Supreme Court ruling 2C_345/2015 of 29 March 2016, E. 6 et seq.
443 FDF Explanatory report 2017a: 15.
444 Report on virtual currencies: 12 et seq.
445 See Reiser 2018: 815 et seq. *inter alia*.
446 FDF Explanatory report 2017a: 15.
447 See FINMA 2018b: 2.
448 Art. 1 para. 2 BankA
449 Art. 1 para. 2 BankA
450 Art. 5 et seq. BankO
451 Art. 5 para. 3 let. a BankO. See also Schönknecht 2016: 312, which states that the wording of this provision is too narrow and that it is not to be understood that general cash payments related to a benefit from the counterparty in an exchange do not come under the term "deposit" (*inter alia*).

Bonds (and comparable debt securities)

The following are not considered deposits: bonds and other standardised debt certificates issued on a large scale; or non-certificated rights with the same function (uncertificated securities), if the creditors are informed to the extent set out in Article 1,156 CO,[452] that is, if a prospectus is (properly) issued and published. This exemption is extended with the entry into force of FinSA. It now applies not only if a prospectus is produced but also if a key information document is issued. If, for example, money is accepted in the context of an ICO (in conventional currency or functionally comparable tokens) and tokens that can be classified as bonds are issued in return, no bank authorisation is required if the conditions mentioned are met.

Settlement accounts

Client assets booked in settlement accounts for the settlement of client business are not considered deposits if no interest is paid and the settlement takes place within 60 days.[453] This exemption does not just apply to securities dealers, precious metal dealers and portfolio managers but also to similar businesses. On the other hand, the exemption does not apply to settlement accounts of foreign exchange dealers.[454]

The Federal Council already established previously that the exemption for settlement accounts can apply specifically to fintech business models[455] and is also valid for tokens if they are classified as deposits.[456] To increase the suitability of the exemption for fintech models and to increase legal certainty, the exemption was amended and extended in 2017 to take account of fintech business models by increasing the settlement period to 60 days[457].

The Federal Council will monitor the effects of the new regulations.[458] To date, no negative repercussions due to the extension of the settlement period have been detected. In discussions with the sector, no acute need for an additional extension has been presented since the entry into force of the extended settlement period (in August 2017). Accordingly, the impact of the new regulations must be monitored further and, if necessary, an amendment of the settlement period may be reconsidered, as has already been suggested by the Federal Council.[459]

Currency dealers today cannot benefit from the settlement account exemption, which means that in practice currency trading is reserved to banks. The same applies to cryptocurrency dealers in accordance with FINMA practice, to the extent that their activity is comparable to that of a currency dealer.[460] However, FINMA currently has enough leeway to apply the exemption provisions of Article 5 paragraph 3 letter c BankO in its consideration of individual cases, especially to blockchain- and DLT-based business models. In this context, the Federal Council will continue to observe further developments.

---

452 See Art. 5 para. 3 let. b BankO

453 Art. 5 para. 3 let. c BankO; FINMA Circ. 2008/3: Margin no. 16.

454 Currency dealers were explicitly excluded from the exemption effective from 1 April 2008, as the non-applicability to currency dealers had led to unsatisfactory results from the point of view of investor protection (see FINMA Circ. 2008/3: margin no. 16.2).

455 FDF Explanatory report Fintech 2017b: 13.

456 FDF Explanatory report Fintech 2017b: 10.

457 The extended settlement period of 60 days should not generally restrict the lengthier settlement periods of securities dealers (or securities firms), see FDF Explanatory report Fintech 2017b: 13; Leimgruber/Flückiger: Margin no. 17.

458 FDF Explanatory report Fintech 2017b: 15.

459 FDF Explanatory report Fintech 2017b: 15.

460 FINMA Circ. 2008/3: Margin no. 16.2.

Money entered into a means of payment or payment system

The following are not considered deposits: monies and functionally comparable tokens that are entered into a means of payment or payment system (e.g. payment cards) in small amounts, are intended solely for the future acquisition of goods or services and do not earn interest.[461] This exemption may be relevant for novel payment services, such as those based on the blockchain. Payment services are normally subject to BankA as client money naturally flows via the operator.[462]

The BankO does not currently specify what "small amounts" are. Based on FINMA practice today, the maximum balance per client and issuer of a means of payment or operator of a payment system must not exceed CHF 3,000.[463] In the opinion of the Federal Council, there is no obvious need at the moment to set a higher limit at regulatory level.

Money with a default guarantee from a bank

Likewise, there is no need for bank authorisation for the acceptance of deposits, provided that a bank subject to the Banking Act guarantees the repayment of the deposits and the payment of the agreed interest (default guarantee).[464] Hence, fintech service providers can also offer custody services for tokens that are functionally comparable to money without bank authorisation, provided that a Swiss bank provides a guarantee in case of default.

Innovation area in banking law (sandbox)

Bank authorisation is only needed by persons that act professionally[465]. Conversely, no bank authorisation is necessary if public deposits are accepted non-professionally.[466] This is the case, for example, when the innovation area (*sandbox*) introduced in 2017 is used. In this case, there is no requirement for bank authorisation even if more than 20 public deposits are accepted or the acceptance of public deposits is advertised. To use the innovation area, the accepted public deposits must not amount to more than CHF 1 million in total[467], and there must be no interest operations.[468] Furthermore, depositors must be notified before they make a deposit that the company in question is not subject to FINMA supervision and that the deposit is not covered by deposit insurance.[469]

This innovation area is designed to meet the needs of fintech business models in particular and thus also blockchain- and DLT-based business models. The parameters of the innovation area – especially the limit of CHF 1 million – were defined with general fintech business models in mind[470] and are not geared specifically to blockchain- or DLT-based business models.

When the innovation area was introduced, the Federal Council stressed that an authorisation-free area also entails risks.[471] In particular, assets accepted in the innovation area are not

461 Art. 5 para. 3 let. e BankO
462 FDF Explanatory report Fintech 2017b: 9.
463 See FINMA Circ. 2008/3: Margin no. 18.1.
464 Art. 5 para. 3 let. f BankO
465 Any party that accepts more than 20 public deposits over the long term or that publicly advertises that it accepts deposits is considered to be acting professionally, even if such advertising leads to fewer than 20 deposits, is considered to be acting professionally within the meaning of BankA. (Art. 6 para. 1 BankO).
466 Art. 6 BankO
467 The limit of CHF 1 million is not to be understood in absolute terms: a company may accept more than CHF 1 million, but it must never post liabilities to clients totalling more than CHF 1 million at any point (e.g. a company accepts CHF 1.5 million during a given period, but pays a total of CHF 0.5 million back to various clients at during the same period.)
468 Art. 6 para. 3 BankO as amended on 1 January 2019
469 Investors must be notified prior to acceptance of the deposit that the provider is not subject to FINMA supervision and that the deposit is not covered by deposit insurance (Art. 6 para. 2 let. c BankO).
470 See FDF Explanatory report Fintech 2017b: 13.
471 See FDF Explanatory report Fintech 2017b: 13.

covered by deposit insurance, as mentioned above. The format of the innovation area is ultimately based on a trade-off between the overall economic benefit and the risks with respect to financial stability and client protection. The maximum amount applicable for the innovation area is intended to be appropriate given the risk involved. The current maximum amount for public deposits in the innovation area is CHF 1 million, which seems insignificant from a systemic point of view. Moreover, the fundamental ban on interest operations specific to banks and the duty to provide information to investors reduce risks in the area of client protection.

The innovation area in banking law has applied since 1 August 2017 and is to be modified in the second quarter of 2019. Consequently, market participants and authorities do not have much experience to date with this instrument. There are currently no compelling reasons for increasing the maximum amount. The Federal Council will duly monitor developments relating to the *sandbox* subject to banking law and make appropriate amendments if it considers necessary in future, for example, due to new blockchain business models.

6.3.2.3 New authorisation category in banking law (fintech authorisation)

In addition to the above elements (expansion of settlement accounts and creation of an innovation area (*sandbox*) subject to banking law), the Federal Council has proposed amending banking law to include a new authorisation category ("fintech authorisation"). Parliament adopted the necessary amendments to BankA on 15 June 2018.

As mentioned above, many fintech business models, including blockchain- and DLT-based models, do not have the time limit transformation typical of banks and thus do not incur the related risks. With the new authorisation category, the authorisation requirements for business models that are limited to the deposit business and do not exceed CHF 100 million in deposits are lower compared with those for banks.[472]

Fintech authorisation gives companies the right to accept public deposits of up to CHF 100 million on a professional basis. This encompasses both traditional currencies (e.g. CHF) and the acceptance of cryptocurrencies (e.g. Bitcoin, Ether). Nonetheless, if cryptocurrencies are accepted for safekeeping and these assets are held on the blockchain and can be attributed to individual clients at all times, these assets are not considered to be deposits[473] and can therefore be accepted by a company with fintech authorisation without regard for the maximum amount of CHF 100 million. Furthermore, companies with fintech authorisation may also hold tokens classified as securities in custody for clients, without needing additional authorisation as a securities dealer or securities firm (in accordance with FinIA) solely for the safekeeping of such securities tokens.[474]

Given the dynamic development of the fintech sector and in particular of blockchain- and DLT-based business models, it is planned that the Federal Council may amend the limit of CHF 100 million. Additionally, FINMA may in exceptional cases make the fintech authorisation available to persons that accept public deposits of more than CHF 100 million on a professional basis or that publicly offer to accept deposits. The requirements set out in BankA apply *mutatis mutandis* to institutions with fintech authorisation. Compliance with these requirements is monitored by FINMA as part of its ongoing supervision.

The new authorisation category comes into force on 1 January 2019. The form of the new fintech authorisation, including the option of increasing the limit to more than CHF 100 million

---

472 As the fintech area and its business models are constantly changing, the new authorisation category is not restricted to specific business models or to the fintech area itself. The fintech authorisation is thus openly formulated and is also available to companies outside the fintech sector that meet the authorisation requirements.

473 See FINMA 2018b: 2.

474 For details on the need for an authorisation as a securities dealer or securities firm, see section 6.5.

on a general or individual basis, seems sufficiently flexible at the moment to be able to react appropriately to future developments. In particular, with effect from 1 January 2019, companies with fintech authorisation can also accept tokens[475] and hold them in custody for clients. The impact of the new fintech authorisation will need to be followed carefully. It will only be apparent how suitable and attractive this new authorisation category is for blockchain- and DLT-based business models when the category comes into force. It will also be necessary to observe closely whether the framework conditions of the fintech authorisation take sufficient account of market developments and whether there is a need for additional regulations, such as a clear indication of which BankA provisions are applicable *mutatis mutandis* to institutions with fintech authorisation and which are not.

6.3.3 Treatment of tokens under bank insolvency law

6.3.3.1 Preliminary remarks

In financial market law, creditor protection plays a key role.[476] This is reflected in the need for authorisation[477] if deposits are accepted and in a specific insolvency regime.[478] The bank insolvency provisions apply not just for banks, but also *mutatis mutandis* to other institutions active in the financial market, such as institutions with fintech authorisation[479], securities dealers and securities firms[480], and financial market infrastructures.[481] If an institution subject to bank insolvency law holds tokens in custody for a client, the question arises as to how such tokens are to be handled under insolvency law.[482] Bank insolvency law distinguishes between deposits and custody assets.

6.3.3.2 Tokens as deposits

If the accepted tokens (e.g. payment tokens such as Bitcoin and Ether) can be classified as deposits, the same bank insolvency rules about the proportionate satisfaction of creditors apply as for the acceptance of deposits in traditional currencies.

6.3.3.3 Tokens as custody assets

The custody assets that can be segregated in favour of the client are set out in BankA and comprise movable assets and securities, as well as certain claims of the custody account holder.[483] The extent to which the term "custody assets" may be interpreted to include tokens with security-like characteristics has not yet been definitively clarified.

In accordance with current legislation, tokens are not considered to be (movable) assets.[484] To the extent that tokens can be classified as securities, the same bank insolvency provisions apply as for traditional securities in the current legal situation, according to the Federal Council. Uncertainties may arise in particular if it is not clear in individual cases whether tokens should be classified as (segregable) securities and/or as (non-segregable) claims. However, this is

---

475 This applies equally to payment tokens, asset tokens and utility tokens.

476 Unlike more recent financial market laws, BankA does not contain a formal purpose clause. The current opinion is that BankA follows a dual purpose, which comprises protecting creditors and the functioning of the financial system (see Müller T.S. 2013: Introduction no. 18; Mauchle 2017: 810 et seq., 813 and footnote 24). The Federal Supreme Court also speaks of "[...] taking into account the main purposes of regulating the financial markets and protecting creditors and investors, as well as the integrity of the financial markets (investor and system protection)", see for example BGE **135** II 345 (360).

477 See in general for example Pulver/Schott 2011: 237 et seq.

478 See section 6.3.2.

479 See Art. 1b BankA (in force from 1 January 2019).

480 Art. 67 FinIA (in force from 1 January 2019).

481 Art. 88 FMIA

482 Regarding general treatment under insolvency law, see section 5.2.

483 Art. 16 BankA

484 See section 5.1.2.4.

not an issue relating to bank insolvency law, but rather a question of what form tokens take in individual cases, as well as their classification under civil and financial market law.

Even in cases in which tokens are classified as custody assets, uncertainties about their segregation under banking law in practice currently remain. One such question is whether or how the procedural provisions on the segregation of custody assets[485] can also be applied to tokens.

6.3.4 Extension of the term "deposit" specifically with respect to tokens?

The term "(public) deposit" is of key significance in banking law both with respect to bank authorisation requirements and in the context of bank insolvency. The question can thus be asked as to whether the term "deposit" under banking law needs to be extended or clarified.

Swiss banking law today uses a broad definition of "deposit", which it then narrows down with a series of exceptional cases.[486] This kind of broad interpretation avoids gaps in definitions, but it has the disadvantage of not being very concrete.[487]

A fundamental revision of the term "deposit" would result in far-reaching amendments to banking law, which would go far beyond the relevance of banking law to blockchain- and DLT-based business models. The legislator could comprehensively revise banking law – including the term "deposit" – but in the past a conceptual approach with a broad deposit definition and specific exceptional cases was deliberately followed. The latest changes to banking law – namely, the innovation area (sandbox), the amendments to settlement accounts and the new fintech authorisation category – are based on this approach, which has proven its worth so far. Given this background, a fundamental conceptual revision of the term "deposit" does not seem appropriate at the moment.

At the same time, it should be noted that in view of the broad scope of the term "deposit", it needs to be clarified for use in practice.[488] The authorisation requirement for the acceptance of public deposits is intended to protect clients from the risk of the counterparty becoming insolvent.[489] If assets (e.g. tokens) are not included in the bankruptcy assets of the custodian or they can be segregated from the bankruptcy assets, there is basically no justification for any special client protection or for the classification of such assets as public deposits.[490] Such a right to segregation already exists in certain conditions today with respect to the transfer of cash.[491] This must also apply in cases in which it is ensured that tokens held in custody (e.g. Bitcoin) are not included in the custodian's bankruptcy assets.

The suggested amendment in DEBA (on the segregability of data, see section 5.2) is intended to further increase legal certainty regarding third-party custody of tokens in insolvency law, which is hence relevant in the context of the term "deposit" under banking law. The reason for this is that if tokens can be segregated from bankruptcy assets in the case of an insolvency, they cannot be classified as deposits from the point of view of banking law and thus there is also no need for bank authorisation.

Where blockchain- and DLT-based business models are structured in such a way that they entail the acceptance of public deposits and no exception applies,[492] the new fintech

485 See Art. 37d BankA.
486 See for example Schönknecht 2016: 300 et seq.; Reiser 2018: 814 et seq.
487 See Schönknecht 2016: 301.
488 See Schönknecht 2016: 301 et seq.
489 See Leimgruber/Flückiger: margin no. 15; Schönknecht 2016: 306, 309.
490 See Leimgruber/Flückiger: margin no. 15; Schönknecht 2016: 309.
491 See Schönknecht 2016: 310.
492 See section 6.3.2.2.

authorisation would be a logical option from 1 January 2019. Public deposits, including deposits in the form of tokens, can be accepted with fintech authorisation.[493]

In view of the above, it does not currently seem necessary to amend the definition of the term "deposit" further specifically with respect to tokens.

6.3.5 Point of contact: Capital requirements for tokens

Banks and securities dealers are obliged to hold certain capital for the assets they hold. The capital requirements also apply for tokens held by banks and securities dealers. The regulatory treatment of tokens with respect to capital requirements is currently being discussed in the Basel Committee.[494] In Switzerland, there are not yet any capital requirements specifically for tokens. Accordingly, FINMA determines the concrete requirements in each individual case. Given the risks associated with tokens (e.g. market risks and operational risks), a conservative risk weighting seems appropriate for tokens, not least to limit the transfer of risks from the area of token-based financial services to the traditional financial sector.

6.3.6 Conclusion

The treatment of tokens and similar assets under bank insolvency law cannot be separated from the general treatment of such assets in the case of insolvency in accordance with DEBA.[495] The provisions under banking law must ultimately be understood as special provisions supplementing DEBA, with DEBA taking a subsidiary role in the context of bank insolvency proceedings.[496] The Federal Council intends to review the treatment of tokens in the case of bank insolvency and to amend BankA in line with the planned amendments to general insolvency law.

6.4 Financial Market Infrastructure Act (FMIA)

6.4.1 Introduction

The Federal Act on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act, FMIA) entered into force on 1 January 2016. It governs the organisation and operations of financial market infrastructures and the rules of conduct of financial market participants in securities and derivatives trading. The purpose of FMIA is to guarantee the functioning and transparency of the securities and derivatives markets, the stability of the financial system, the protection of financial market participants and the equal treatment of investors.[497]

The current version of FMIA is based on a traditional picture of centrally organised financial market infrastructures,[498] which can result in unanswered questions or a need for action in a primarily decentralised environment.[499] With respect to blockchain- and DLT-based applications, the central definitions of "securities" and "derivatives" in financial market regulations,[500] regulations on financial market infrastructures[501] and market conduct rules[502] are particularly relevant.

---

493 See section 6.3.2.3.
494 See section 4.2.
495 See section 5.2.
496 Art. 34 para. 2 BankA
497 See Art. 1 FMIA.
498 For example, stock markets and other trading facilities concentrate buy and sell offers in a *central office* (see Dispatch regarding FMIA, 7489); FINMA regulates *central* counterparties (Art. 48 et seq. FMIA) and *central* custodians (Art. 61 et seq. FMIA).
499 See section 6.4.7.3.
500 See section 6.4.2.
501 See section 6.4.6.
502 See section 6.4.8.

6.4.2 Securities and derivatives terms in financial market infrastructure law

6.4.2.1 Background

The legal definitions of "securities" and "derivatives" are of key importance in financial market law. Additionally, both terms are relevant for blockchain- and DLT-based business models. Two key questions can be asked in this connection: firstly, whether or which tokens fall under these definitions; and secondly, to what extent these definitions in their current form match novel, token-based financial instruments.

Certificated and uncertificated securities, derivatives and intermediated securities that are standardised and suitable for mass trading are considered to be securities. Certificated and uncertificated securities, derivatives and intermediated securities are standardised and suitable for mass trading if they are publicly offered for sale in the same structure[503] and denomination or are placed with more than 20 clients, insofar as they have not been created especially for individual counterparties.[504]

The term "securities" was defined in SESTA before the introduction of FMIA and has not been amended since SESTA entered into force. Legal studies have criticised the term "securities" in some instances.[505] On the introduction of FMIA, the term "securities" was reviewed. The Federal Council stated its opinion in 2015 that the term "securities" in SESTA had proved effective in practice and that it should be used in FMIA unchanged; however, the term "intermediated securities" was added to the term "securities".[506] At that time, there was no need to call the term "securities" into question with respect to blockchain- and DLT-based business models. Accordingly, the current term "securities" in FMIA (and in future also in FinSA) is a continuation[507] of the earlier definition in SESTA.[508]

The legal implications of the classification of a financial instrument as a security are derived from the relevant financial market laws and apply above all to the secondary market.[509] Hence, provisions about trading venues are only relevant for products that are classified as securities.[510] The same applies for authorisation requirements and rules of conduct for securities dealers in accordance with SESTA (or in future authorisation requirements for securities firms in accordance with FinIA).[511] The term "securities" is also to be found in the market conduct rules: insider information must refer to securities, and the object of market and price manipulation must be a security.[512]

---

503 E.g. regarding duration, interest rate, etc.

504 Art. 2 let. b FMIA; Art. 2 FMIO. Also in future Art. 3 let. b FinSA.

505 For example, the previous vagueness will remain, with certificated securities, uncertificated securities and intermediated securities designating the civil law form, while the term "derivatives" refers to the content of a law (Favre/Kramer 2017: Art. 2 let. b FMIA no. 5).

506 See Dispatch regarding FMIA dispatch, 7513.

507 See Dispatch regarding SESTA: 1369 et seq.

508 The definition was extended to include intermediated securities that are standardised and suitable for mass trading in the term "securities" (see Dispatch regarding FMIA, 7513).

509 The issue of securities in the primary market is not subject to authorisation requirements. The same applies to the public offering of securities. Authorisation may be required if a party issues derivatives itself and offers them publicly for its own account or for the account of others in the primary market, (Art. 3 para. 3 SESTO), or if tokens classified as securities are acquired on a firm basis or on commission by third parties and offered publicly in the primary market for the first time (Issuing house activity, Art. 3 para. 2 SESTO. In future, these activities will be reserved to securities firms and banks (see Art. 44 FinIA). Details on prospectus requirement, see section 6.6.5.1.

510 See Art. 26 FMIA.

511 See Art. 1 et seq. SESTA or in future Art. 41 et seq. FinIA.

512 See Art. 142/154 FMIA (regarding insider information) and Art. 143/155 FMIA (regarding market manipulation); more in Favre/Kramer 2017: Art. 2 let. b FMIA no. 19.

A derivative is a financial contract whose value depends on one or more underlying instruments and which does not constitute a cash transaction.[513] Neither the act nor the ordinance defines "financial contract". In the dispatch, financial contracts are referred to as "bilateral agreements".[514] Hence, a generally formulated definition of derivatives applies in FMIA, with individual products in a "negative list" excluded from its scope.[515] Unlike the situation with the term "securities", it is not significant for classification as a derivative whether the instrument is standardised and suitable for mass trading. The term "derivative" has at times been criticised in legal studies as in need of interpretation.[516]

6.4.2.2 The term "securities" in the case of tokens

As explained, tokens are not certificated securities, but may be classified as uncertificated securities, derivatives or, under certain circumstances, as intermediated securities.[517] As the definition of securities is neutral with respect to technology, tokens may be classified as securities.[518] If tokens are classified as securities, authorisation as a securities dealer (or securities firm) is needed[519] for commercial trading with such tokens, and the trade of such securities-tokens on a platform is subject to specific requirements. The classification of tokens as securities gives rise to various questions, primarily with regard to the secondary market (e.g. crypto trading platforms).

Firstly, it is not immediately obvious which tokens can be classified as securities. As FINMA indicated in its guidelines, there are differing opinions in legal studies, given the current definition of "securities", as to whether all tokens represent uncertificated securities and therefore may be classified as securities.[520] According to current practice, FINMA generally[521] rejects the classification of both payment tokens and utility tokens as securities. The reason for this is that payment tokens are intended as a means of payment and so they do not present any similarities to traditional securities based on their economic function. Likewise, utility tokens are not analogous to securities because there is no connection to the capital market.[522] By contrast, FINMA considers asset tokens to be securities if they represent an uncertificated security and are standardised and suitable for mass trading.[523]

Secondly, due to the flexible form of tokens, they cannot be classified in a uniform manner under financial market law in all circumstances. As token classifications[524] are not mutually exclusive, tokens could be classified as securities and payment means at the same time ("hybrid tokens"), which results in a cumulative application of the corresponding requirements under financial market law.

There is also a time dimension. Depending on the form of the ICO, tokens can be issued either on the raising of funds or after the raising of funds and must therefore be treated differently under financial market law. In particular in the case of ICOs, there may frequently be changes of the legal status attributed to the tokens issued due to the fast-moving nature of many business models used by ICOs, and thus there may also be a change in the legal classification

---

513 See Art. 2 let. c FMIA; Art. 2 para. 2 FMIO.
514 See Dispatch regarding FMIA dispatch, 7513.
515 See Favre/Kramer 2017: Art. 2 let. c FMIA no. 2; see Art. 94 para. 3 FMIA; Art. 2 para. 3 FMIO; Art. 80 FMIO.
516 See Favre/Kramer 2017: Art. 2 let. c FMIA no. 5 *inter alia.*
517 See section 5.1.2.
518 See FINMA 2018a: section 3.2.
519 See section 6.5.
520 See FINMA 2018a: section 3.2.1.
521 In the case of prefinancing and presales, rights to the future purchase of tokens can be classified as uncertificated securities, which must be treated as securities (see FINMA 2018a: no. 3.2.3). Furthermore, hybrid tokens remain reserved.
522 See FINMA 2018a: section 3.2.1 / 3.2.2.
523 See FINMA 2018a: section 3.2.3.
524 See section 6.2.

of the tokens in question. Based on FINMA practice, this may mean that such tokens acquire the character of securities at some date and that the same tokens later lose this property again (or vice versa). The changing legal classification of tokens over time may mean that the market participants involved are subject to different or additional duties (e.g. professional trading with tokens classified as securities requires authorisation as a securities dealer or, under FinIA, as a securities firm). From the point of view of the token issuer, classification of the token as a security may be undesirable, as this can make it more difficult for such tokens to be accepted for trading on crypto trading platforms[525]. The same applies in the case of a change in the legal status of tokens over the course of time.

As a result, it can be stated that the current financial market infrastructure law can lead to specific challenges in the case of blockchain or DLT-based business and financing models, such as those that underlie numerous ICOs today. The reason for this is, firstly, the considerable flexibility in the content-related design of tokens. Secondly, the flexibility in token design also has a time dimension, meaning that tokens can be functionally very dynamic instruments.

6.4.2.3 The term "derivatives" for tokens

Tokens can have very flexible forms, which in some cases results in their value depending economically on another underlying asset. In the case of forward transactions, such tokens can be classified as derivatives.[526] In current FINMA practice, derivatives set up as tokens have only rarely been seen to date.

Unlike a classification as a security, a classification as a derivative has a more significant impact on proceedings in the primary market. Any party[527] that creates standardised derivatives itself that are suitable for mass trading and offers them publicly in the primary market for its own account or the account of third parties is considered under prevailing law as a derivatives firm and needs authorisation as a securities dealer.[528] In accordance with the future provisions in FinIA, the professional creation of derivatives (in the form of securities) for public offering on the primary market will also be reserved to banks and securities firms – and thus to institutions subject to FINMA supervision.[529] Accordingly, the creation and public offering of such token derivatives classified as securities may need authorisation. From the point of view of current practice, there is no clear need for other market participants (subject to FINMA supervision) to create and offer token-derivatives professionally. Given this background, it does not currently seem appropriate to give other players access to the activity that is reserved to banks and securities firms in accordance with FinIA.

The classification of tokens as derivatives also has an impact on the secondary market: specific market conduct rules[530] were set out in FMIA for certain derivative transactions, including transaction reporting to trade repositories, transaction clearing via central counterparties and risk mitigation measures. The market conduct rules correspond to international standards and comparable regulations in other jurisdictions and apply to financial and non-financial counterparties with their registered office in Switzerland.[531] Nonetheless, such market conduct rules were not drafted with novel derivatives in the form of tokens in mind either inside or

---

525 In this context, the term "listing" is often used in a non-technical manner, but this cannot be considered equivalent to listing on a stock exchange.

526 The situation is different for (traditional) derivatives that have a token as their underlying asset.

527 Art. 3 para. 3 SESTO.

528 An independent economic activity aimed at making long-term earnings is considered to be professional (see *inter alia* Art. 3 FinIA).

529 Art. 12 let. b FinIA.

530 See Art. 93 et seq. FMIA.

531 Art. 93 para. 1 FMIA, whereby only legal entities recorded in the Swiss commercial register (and some economically active foreign companies) can be classified as non-financial counterparties, see Art. 77 FMIO.

outside Switzerland, but instead are intended to regulate traditional forms of exchange-traded and OTC derivatives. One illustration of this is the clearing duty. Counterparties in derivatives trading must use an approved or recognised central counterparty to clear derivatives that are not traded via a trading venue.[532] In a fully decentralised DLT or blockchain system, however, central clearing seems to run counter to the nature of the system.

A thorough review of the definition of derivatives applicable in Swiss financial market law with respect to blockchain technology and tokens would be one-sided and incomplete, and it should thus be embedded in a more comprehensive context.

6.4.2.4 Interim conclusion: no amendment of the definitions of securities and derivatives

The question can be asked as to whether an amendment to the current definition of securities is justifiable in view of blockchain- and DLT-based business models. Making the definition of securities more flexible would facilitate secondary trading with tokens that are also classified as securities, as the provisions on securities trading would no longer have to be observed. However, this kind of approach would primarily entail risks: risks in the areas of investor protection and the reputation of the Swiss financial market; risks relating to the equivalence of Swiss financial market law provisions to foreign requirements; the risk of being treated unequally without good reason compared with financial market players that do not use blockchain technology; and opportunities for regulatory arbitrage via the use of blockchain technologies.

Instead of making the definition of securities more flexible, the creation of a new legal definition specifically for securities in the form of tokens could be envisaged in FMIA and FinSA. This approach would, however, be a departure from the principle of technology-neutral regulation. Moreover, merely setting out a new legal definition of a securities token would not suffice. Financial market law would in this case have to define which requirements that are generally applicable to securities should apply equally to securities in the form of tokens, which should apply analogously and which should not apply to such token securities. This would result in the creation of comprehensive and complex technology-specific token regulation.

In the opinion of the Federal Council, the current legal definitions for securities and derivatives have proved useful, and it is not essential to change them. Blockchain- and token-based applications specific to the financial sector should be able to develop in a framework that allows and fosters innovation. At the same time, fundamental goals under financial market law, such as the protection of investors, creditors and the integrity of the Swiss financial market, must be maintained. Existing challenges in the classification of tokens can be clarified by means of forward planning and consultation, as well as by means of current tools (e.g. queries about which laws apply; FINMA no-action letters). Where the issues involve secondary trade with tokens, these must be dealt with directly and specifically.[533]

6.4.3 Financial market infrastructures in the age of blockchain and DLT

Since 1 January 2016, financial market infrastructures have been uniformly regulated by FMIA. FMIA governs the operation of financial market infrastructures (FMIs) and obligations in trade with securities and derivatives. Financial market infrastructures are of crucial significance today for smoothly operating financial markets. They make it possible to standardise, automate and accelerate the various steps in processing a securities transaction (trade, clearing,

---

532 Art. 97 FMIA. The aim of the central clearing duty for OTC derivatives is firstly to reduce the counterparty default risk for both parties and secondly to lower the risk of contagion on the default of a participant and thus strengthen financial stability.

533 See section 6.4.4.

settlement and reporting). They make a key contribution to the efficiency and stability of the financial system.

FMIA counts stock exchanges, multilateral trading facilities, central counterparties, central securities depositories, payment systems and trade repositories as financial market infrastructures.[534] The current regulation is based on a scenario of centrally organised infrastructure. An example is the stock exchange, which acts as a market place, bringing together supply and demand, and so becomes an institutionalised, *central* trading venue.[535]

The regulation of financial market infrastructures faces various issues regarding trade with tokens, which can be divided into two main topics.

- The first topic addresses the many points of contact between the current (central) financial market infrastructures and novel, token-based instruments. This area concerns, among other things, interfaces between the current (traditional) financial system and blockchain- or DLT-based business models. Various questions can be raised in this context. At what conditions can financial instruments be traded at trading venues?[536] This would also depend on the definition of securities.[537] Can the operation of a blockchain-based securities system be classified as a payment system?[538]
- The second topic concerns the core of today's financial market infrastructures. If financial markets are organised increasingly by decentralised "infrastructures" (e.g. smart contracts) in the future, difficult questions arise: What risks and opportunities do such decentralised structures present for investor protection, as well as for the integrity and stability of the financial markets? What must or might the regulation of such decentralised financial market infrastructures involve?[539] Hence, the current developments in the area of innovative financial technologies – namely in the areas of DLT and blockchain – are also sparking a need for action in the regulation of financial market infrastructures.

Developments in the area of blockchain and DLT are causing a specific issue in financial market infrastructure law. Today, a legal entity may only operate one financial market infrastructure.[540] The only exception is for the operation of a multilateral trading facility by a stock exchange. The developing business models in the area of blockchain and DLT show that this requirement is a potentially unnecessary barrier to market entry. At the same time, it does not seem appropriate to remove this requirement, given the situation in "traditional" financial market infrastructures. In view of the considerable momentum in the area of blockchain and DLT, the Federal Council proposes accordingly that the current regulations should be maintained and made more flexible at the same time, so that exceptions from a provision anchored at legislative level (e.g. a legal entity may operate only one financial market infrastructure) may be granted in justified cases. This requires an amendment to FMIA and an amendment to FMIO.

534 Art. 2 let. a FMIA.
535 For the economic background and definitions of "stock exchange", see in particular Schott A./Winkler 2017: Art. 26 FMIA no. 4 et seq.
536 See section 6.4.4.
537 See section 6.4.2.
538 See section 6.4.5.
539 See section 6.4.7.3.
540 Art. 10 FMIA; the foregoing does not apply to the operation of a multilateral trading facility by a stock exchange.

6.4.4 Trading institutions

6.4.4.1 Overview

Trading institutions for financial instruments are of fundamental importance because they bring together supply and demand. FMIA defines three types of trading institution: stock exchanges, multilateral trading facilities (MTF) and organised trading facilities (OTF).[541] Stock exchanges and MTFs are combined under the term "trading venue".[542] The term "trading institution" is not used in FMIA. It will be used hereinafter to refer to all institutions for the trading of securities, e.g. stock exchanges, MTFs and OTFs. FMIA uses the following definitions:

- *Stock exchanges:* institutions for multilateral securities trading where securities are listed; a stock exchange permits the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules;
- *Multilateral trading facilities* (MTFs): institutions for multilateral securities trading whose purpose is also the simultaneous exchange of bids between several participants and the conclusion of contracts based on non-discretionary rules but without listing securities;
- *Organised trading facilities* (OTFs):[543] institutions for multilateral or bilateral trading in securities and other financial instruments based on discretionary or non-discretionary rules.

Trading institutions can be differentiated according to various criteria, for example, based on authorisation requirements (or on authorisation categories), on types of trade, on the financial instruments that can be traded at the trading institution, and permissible trade participants.

The trading institutions regulated in FMIA can be summarised as follows:

<table>
<tr><th></th><th>Stock exchange</th><th>Multilateral trading facility (MTF)</th><th>Organised trading facility (OTF)</th></tr>
<tr><td>Authorisation necessary</td><td>Yes</td><td>Yes</td><td>Indirectly (operations only via a bank, a securities dealer or a trading venue) – no separate authorisation category as OTF</td></tr>
<tr><td>Type of trade</td><td colspan="2">Multilateral</td><td>Multilateral or bilateral</td></tr>
<tr><td rowspan="2">What is traded</td><td colspan="2">Securities</td><td rowspan="2">• Securities and
• other financial instruments</td></tr>
<tr><td>Listed</td><td>No listing</td></tr>
<tr><td>How trade is carried out</td><td colspan="2">Non-discretionary rules</td><td>• Discretionary rules
• Non-discretionary rules</td></tr>
<tr><td>Who can participate</td><td colspan="2">Only (in accordance with the regulations of the trading venue)
• Securities dealers (or securities firms)
• Parties subject to FINMA supervision</td><td>No restrictions (i.e. also retail clients)</td></tr>
</table>

541 See Art. 26 et seq. FMIA on stock exchanges and MTF; Art. 42 et seq. FMIA on OHS.
542 Art. 26 let. a FMIA.
543 See also FINMA Circ. 2018/1.

	Stock exchange	Multilateral trading facility (MTF)	Organised trading facility (OTF)
	• Foreign participants authorised by FINMA • SNB		

Table 2: Overview of trading institutions

Secondary trade with tokens can present various points of contact with FMIA regulations on stock exchanges, multilateral trading facilities and organised trading facilities. These include

- authorisation requirements for such trading facilities (Article 6.4.4.2);
- the assets tradeable via such facilities (Article 6.4.4.3);
- the trading facilities' obligations (Article 6.4.4.4);
- regulations about access to these trading facilities (Article 6.4.4.5);
- the obligations applicable to these trading participants (Article 6.4.4.6).

6.4.4.2 Licensing requirement for crypto-trading platforms

Stock exchanges and MTFs need financial market infrastructure authorisation from FINMA.[544] No special authorisation is required to operate an OTF. However, OTFs can only be operated by authorised banks, securities dealers, trading venues and financial groups subject to consolidated supervision by FINMA. All of these financial market participants are supervised by FINMA in any case.[545]

The operation of a trading platform for tokens classified as securities needs authorisation. By contrast, operation of a trading platform for non-securities (e.g. pure payment tokens) does not require authorisation as a financial market infrastructure.[546]

The operation of exchange platforms (e.g. crypto-brokers) and distributed *peer-to-peer* platforms must be distinguished from the operation of a *centralised* trading platform for tokens. In the current legal situation, there is no authorisation requirement for exchange platforms and distributed peer-to-peer platforms in accordance with FMIA. By contrast, the operation of a *decentralised* trading platform for securities tokens requires authorisation pursuant to FMIA in the current legal situation.

544 Art. 26 in conjunction with Art. 4 para. 1 in conjunction with Art. 2 let. a no. 1 or 2 FMIA.
545 Art. 43 para. 1 FMIA.
546 For details on the regulation of payment systems, see section 6.4.5. For details on authorisation as a bank, see section 6.2.

The current legal situation for trade with tokens in the secondary market can be summarised as follows (*Table 3: Trade with tokens in the secondary market area*):

	Classification pursuant to FMIA	**Other**
Exchange platforms /crypto-brokers	No authorisation requirement pursuant to FMIA.	If the operator also offers custody services, it must be examined whether such services are subject to the Banking Act or whether fintech authorisation should be obtained. If such brokers trade with tokens that are classified as securities, authorisation for securities dealers (securities firms) may be necessary.
Centralised trading platforms	The operation of such platforms may require authorisation pursuant to FMIA, if the tokens traded on the platform qualify as securities.	If such platforms also offer their clients account administration (e.g. for margin settlement) and hold the cryptocurrencies in pooled accounts on the blockchain, it must be examined whether BankA applies. The fintech authorisation, which comes into force on 1 January 2019, may, however, be worth considering for such service providers.
Decentralised trading platforms	The operation of this kind of platform may be subject to authorisation in accordance with FMIA.	
Distributed or peer-to-peer platforms	The operation of this kind of platform is *not* subject to any authorisation requirements today in accordance with FMIA, irrespective of whether the transactions brokered on the platform are related to securities.	

In the Federal Council's view, it is not currently clear why the operation of a trading platform for securities in the form of tokens should be regulated differently in terms of authorisation requirements than a trading platform for traditional securities without any connection to the blockchain. Accordingly, a general exemption from the authorisation requirement for crypto exchanges and crypto trading platforms in the area of securities does not seem necessary, given the protective purpose of FMIA.

For the operation of blockchain-based trading platforms for tokens classified as securities, the question arises as to which type of authorisation is appropriate for the following cases:

- Stock exchange or MTF authorisation is necessary for multilateral trade in securities in accordance with *non-discretionary* rules (i.e. without discretionary decisions by the platform operator). In view of their automation via *smart contracts*, non-discretionary systems are probably the usual scenario for blockchain-based trading platforms, as far

as can be seen today. Access to a stock exchange or MTF is currently limited to authorised financial market institutions. This means that retail clients – who are often the target group for today's blockchain-based trading platforms – are excluded from such platforms.[547] Hence, business models that are geared directly to retail clients and intended for multilateral trade in securities in accordance with non-discretionary rules cannot be granted authorisation under current legislation, but they likely correspond to a need.

- *Discretionary multilateral* and *bilateral* trade in tokens classified as securities does not need separate FMIA authorisation. However, operation of an OTF for such trade is reserved to banks, securities dealers, trading venues and financial groups subject to consolidated FINMA supervision. Problems may arise today, for example, if authorisation holder wishes to operate an OTF (e.g. for tokens classified as securities) and requests an authorisation from FINMA (e.g. as a securities dealer) for this purpose only. In accordance with current practice, the operator would in this case not be eligible for authorisation.

Given this background, the Federal Council proposes an extension of the authorisation requirements applicable to securities firms. Specific amendments to the statute and corresponding provisions in the ordinance should make it possible for market participants to apply for authorisation in the future, even for the (sole) purpose of operating an OTF. Additionally, it must be examined in due course whether the operation of an OTF should be permitted for the persons specified in Article 1b BankA (fintech authorisation). This analysis must be based on initial experience with the new authorisation category, which enters into force on 1 January 2019.

Finally, there is the question of whether the operation of trading facilities for payment tokens or other tokens classified as non-securities should be subject to authorisation. At present, a new authorisation requirement of this kind does not seem necessary. The operation of a trading platform for means of payment that are *not* securities is not subject to a specific authorisation requirement in FMIA in the "analogue" world either. At least there is a provision in FMIA on payment systems, and therefore it is also possible to make payment systems subject to FINMA authorisation if this is necessary for the proper functioning of the financial market or for the protection of financial market participants.[548] The option of an OTF is available today for platforms intended for multilateral trading[549] of financial instruments that are not classified as securities.

6.4.4.3 Assets traded in trading facilities

Another topic involves the issue of which assets can be permitted in trading facilities.

- **Securities:** Stock exchanges and MTFs are geared and at the same time restricted to securities at present. Accordingly, it is already possible for stock exchanges and multilateral trading facilities to permit trade in crypto-based assets that are classified as securities. The corresponding authorisation requirements must be set out in regulations drawn up by the trading venue.[550] The regulations must be approved by FINMA.[551] Organised trading facilities may also allow securities to be traded. They are more

547 See section 6.4.4.5.
548 See section 6.4.5; see also Art. 4 para. 2 in conjunction with Art. 81 et seq. FMIA.
549 In accordance with both discretionary and non-discretionary rules, see Art. 42 let. a and b FMIA.
550 Art. 35 FMIA (for stock exchanges) and Art. 36 FMIA (for multilateral trading facilities).
551 Art. 27 para. 4 FMIA.

flexible than both stock exchanges and multilateral trading facilities[552], by being able to offer bilateral as well as multilateral trade with securities.[553]

- **Non-securities:** Stock exchanges and multilateral trading facilities within the meaning of FMIA primarily accept securities for trading, On the other hand, stock exchanges and multilateral trading facilities may also operate an organised trading facility for the purpose of multilateral trade with financial instruments that are not securities.[554] FMIA focuses solely on trade with securities or other financial instruments. It does not expressly specify whether stock exchanges, multilateral trading facilities and organised trading facilities may accept other assets for trading (e.g. payment tokens, such as Bitcoin, Ether, etc.). Consequently, in accordance with applicable regulations, stock exchanges, MTFs and OTFs are free to also accept non-securities that are not financial instruments (e.g. Bitcoin, Ether, etc.) for trading, provided that the relevant regulations (e.g. on organisation, fit and proper, ancillary services, IT systems) are observed.[555]

6.4.4.4 Duties of trading institutions

FMIA sets out the duties to be met by financial market infrastructures.[556] It specifies general requirements (e.g. organisation and management, risk management, fit and proper business conduct, outsourcing, business continuity, minimum capital requirements, operation of IT systems, documentation and storage duties, avoidance of conflicts of interests, etc.). These requirements apply to all financial market infrastructures. Moreover, FMIA sets out specific, additional requirements for individual financial market infrastructure types; for trading venues in particular the additional requirements concern the transparency of trade, guaranteeing of orderly trade and monitoring of trade.

The requirements for trading institutions applicable in the traditional financial world seem to be appropriate today for trading institutions in the area of blockchain and DLT too, provided that such institutions are centrally organised – like traditional financial market infrastructures – and pursue similar business activities.[557] The provisions requiring trading venues to have a minimum level of capital (currently CHF 1 million)[558] seem basically appropriate.

It must, however, be conceded, that certain provisions of financial market infrastructure law are not always suitable for blockchain- or DLT-based financial market infrastructures. For example, the provisions to guarantee orderly trade currently state that trading venues must have the necessary systems and procedures to cancel, alter or rectify each transaction in exceptional cases.[559] Based on the system properties of blockchain- and DLT-based systems, namely their irreversibility[560], such a requirement cannot be readily met by a blockchain or DLT system. At the same time, the removal of this requirement for all trading venues cannot be justified. To take into account the specific properties of blockchain and DLT systems nonetheless, approaches that are functionally equivalent but more flexible need to be found. To improve flexibility, the Federal Council's concrete proposal is to make an amendment to

552 But currently only in accordance with discretionary rules (see Art. 42 let. a. FMIA).
553 Art. 42 FMIA; see also FINMA Circ. 2018/1: margin no. 24 et seq.
554 See Art. 43 para. 1 FMIA; Art. 10 para. 1 sentence 2 FMIA.
555 If such platforms offer their clients accounts as well, an authorisation as a bank or fintech authorisation would also be necessary in certain circumstances.
556 See Art. 4 et seq. FMIA (general duties); Art. 26 et seq. FMIA (specific duties for trading facilities). Furthermore, special requirements apply for systemically important financial market infrastructures (Art. 22 et seq. FMIA).
557 For details of the development of decentralised financial market "infrastructures", see section 6.4.7.
558 Art. 13 para. 1 let. a FMIA (or CHF 1.5 million in justified cases).
559 See Art. 30 para. 2 let. f FMIO.
560 See section 2.1.

FMIO that would give FINMA the power to grant exemptions from this requirement, provided that such exemptions do not run counter to the purpose of the law.[561]

Additionally, prevailing financial market infrastructure law contains various written form requirements, which should also be made more flexible, in the Federal Council's opinion.[562] Both traditional and blockchain trading institutions would benefit from such amendments. Such specific changes would make the requirements in financial market infrastructure law better suited to digital business models and thus to blockchain- and DLT-based systems.

Blockchain/DLT technologies and their applications in the area of finance are still at an early stage, and their development is extremely dynamic. Accordingly, it is feasible that ongoing regulatory adjustments may be needed, depending on the future development of blockchain/DLT and their applications. A new authorisation category is being proposed for financial market infrastructures in the area of blockchain, in view of this rapid, dynamic development and the increasingly evident specific needs in this area.[563]

6.4.4.5 Market players participating in trading institutions (participants)

Another pertinent question is who may participate in a trading institution. It must be clarified whether access to trading institutions in the area of crypto-based assets should be limited to specific participants or remain open, so that, for example, private clients ("retail clients") can also participate. In particular, this affects the multilateral trading of securities in accordance with non-discretionary rules (i.e. without discretionary decisions by the operator).

Today, stock exchanges and multilateral trading facilities are only open to securities dealers (or securities firms in accordance with FinIA), other parties supervised by FINMA in accordance with Article 3 FINMASA[564] (provided that the trading venue ensures that they meet equivalent technical and operational conditions to those applicable to securities dealers), foreign participants authorised by FINMA and the SNB.[565] Institutions with fintech authorisation may also be permitted to participate in such trading venues from 1 January 2019 if they meet the conditions set out in FMIA. However, there are no provisions for direct access by other market players, such as private clients. In contrast to the restrictions for stock exchanges and multilateral trading facilities, FMIA does not contain any restrictions on participant access for organised trading facilities.

The reason for limiting the kinds of participants in stock exchanges and multilateral trading facilities is to protect investors and the proper functioning of the financial markets.[566] In this context, it should be noted that the participants admitted to a trading venue must fulfil specific duties in securities trading, i.e. a duty to keep records of the orders and executed transactions, as well as reporting duties.[567]

The current provision on the (limited) participant group for trading venues has proved its worth so far, and there does not currently seem to be any need for further flexibility. At the same time, the attractiveness of Switzerland as a location for financial market infrastructures for crypto-based assets (e.g. crypto trading platforms) depends on such platform providers being able to reach as broad a client base as possible. For trade with tokens via blockchain- or DLT-

561 Comparable exemption provisions can be found in Art. 29 para. 2 FMIO and Art. 127 para. 2 FMIO.
562 For example regarding the agreement between the trading venue and participants with a specific function (Art. 30 para. 3 FMIO) or regarding the agreement on the outsourcing of activities to a service provider (Art. 11 para. 2 FMIA).
563 See section 6.4.7.2.
564 Art. 34 para. 2 let. b FMIA.
565 Art. 34 FMIA. The provisions on permissible participants are therefore similar to those in EU law (see Dispatch regarding FMIA, 7535).
566 See for example Truffer 2011, Art. 7 SESTA no. 11 *inter alia*
567 See section 6.4.4.6.

based platforms, a "roundabout" route via regulated participants for technical reasons is no longer necessary. Greater flexibility of the participant group, for example for multilateral trading facilities, would raise a number of questions, however, and lead to additional regulatory needs. For example, it would be necessary to regulate which duties are incumbent on such participants,[568] how to differentiate between duties for professional and non-professional participants, and whether it would even be feasible to impose (new) duties on non-professional trade participants. Given this background, the creation of a new authorisation category in the financial market infrastructure area is proposed below, rather than an amendment to today's rules for trading venues.[569]

6.4.4.6 Duties of the participants in trading facilities

In accordance with the current legal situation, participants permitted to trade at a Swiss trading venue (stock exchange or multilateral trading facility) have two primary duties in this capacity:[570] Firstly, they must record the orders and the transactions they carry out with all details necessary for the traceability of the said transactions and the supervision of their activity. Secondly, participants must make the disclosures necessary for the transparency of securities market trading.[571] These duties were extended by FMIA to all participants in a trading centre, as well as to derivatives based on securities that are admitted for trading at a trading venue. There is now also a requirement for details to be provided to identify the beneficial owner.[572] This is essential for the effective combating of market abuse (insider trading and market or price manipulation). The EU has a comparable regulation.[573]

The aims behind the record-keeping and reporting duties also apply to trade with tokens if they are classified as securities. It must be asked, however, to what extent these duties in their current form are suitable for trading with token-based securities or whether – in view of the specific form of token-based securities – certain (technical) adjustments are necessary, for example to the reporting duty in securities trading.

A fundamentally more flexible approach to the duties incumbent on the participants permitted to trade at a trading venue does not seem appropriate, however, as the duties have just been stepped up and brought into line with international standards with the entry into force of FMIA. In this context – and also with a view to making the group of permitted trade participants more flexible – it seems more expedient to create a new authorisation category.[574] This approach creates greater flexibility with respect to the duties of trade participants, without calling current duties in securities trading into question. This would make it possible to make admission criteria (who is permitted to take part in a trading facility) somewhat more flexible.

6.4.5 Payment systems

FMIA defines a payment system as "an entity that clears and settles payment obligations based on uniform rules and procedures".[575] FMIA regulation of payment systems is not restricted to legal tender (coins issued by the Confederation, banknotes issued by the SNB

568 See section 6.4.4.5.
569 See section 6.4.7.
570 Art. 38 et seq. FMIA; Art. 36 et seq. FMIO; Art. 1 et seq. FMIO-FINMA; FINMA Circ. 2018/2 (Duty to report securities transactions). See also FINMA Circ. 2013/8 (Market conduct rules).
571 See Art. 38 et seq. FMIA; Art. 36 et seq. FMIO; FINMA Circ. 2018/2.
572 Art. 37 FMIA.
573 See FDF Explanatory report FMIO 2015: 23.
574 See section 6.4.7.2.
575 Art. 81 FMIA.

and sight deposits with the SNB). Hence, the definition of payment system in FMIA does not exclude the use of payment tokens (crypto currencies).[576]

A crypto payment system may be seen as a payment system within the meaning of FMIA. That applies both for a central payment system with payment tokens and for a decentralised payment system. Nonetheless, FMIA is by its very nature not designed for decentralised payment systems. Payment systems subject to authorisation must meet various requirements, in particular regarding organisation, minimum capital, business continuity and the publication of information.[577] Some of these are fundamentally unsuited to a decentralised payment system. By contrast, a central crypto system should be able to meet these requirements. A partially decentralised payment system (e.g. decentralised validation) should also be able to meet the requirements if there is an "operator" that can define the rules of the operation of the payment system.

In practice, no payment system has so far needed an authorisation pursuant to FMIA. Any authorisation requirement for a crypto payment system will depend on its future significance for payment transactions between financial market participants in Switzerland. Authorisation is only required if it is necessary for the functioning of the financial markets or for the protection of financial market participants. The FMIA dispatch gives as examples a systemically important bank and a payment system that handles financial transactions between financial intermediaries. A payment system operated by a bank (e.g. PostFinance) or a payment system operated by or on behalf of the SNB (e.g. Swiss Interbank Clearing) does not need authorisation pursuant to FMIA.[578]

6.4.6 Clearing and settlement systems

a) Preliminary remarks

FMIA stipulates additional financial market infrastructures for the post-trading settlement of securities transactions. This includes in particular central counterparties[579] and central securities depositories[580]. These infrastructures ensure in applying CC and FISA in particular that securities traded via trading venues and OTFs can be transferred and deposited securely. So-called post-trading infrastructures also include payment systems described above.[581]

With respect to novel decentralised settlement and/or depository systems for tokens with the characteristics of securities, the question arises whether, for example, settlement via smart contracts can be classified in material terms as financial market infrastructure and, if so, what the implications of this would be.

b) Central counterparties

A central counterparty is an entity that interposes itself according to specific rules and procedures between the counterparties to a securities transaction, thereby becoming the buyer to every seller and the seller to every buyer. It also nets counterpositions. Central counterparties are subject to authorisation as a financial market infrastructure.[582]

---

576 This opinion is also put forward by Bärtschi/Meisser 2015: 119 and Hess/Kalbermatter/Weiss Voigt 2017: Art. 81 FMIA no. 22 et seq. In accordance with the classification of ICOs in FINMA 2018a, payment tokens are "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 asset transfer".

577 Art. 8 et seq. FMIA.

578 Art. 4 para. 2 and para. 3 FMIA.

579 Art. 48 et seq. FMIA.

580 Art. 61 et seq. FMIA.

581 Art. 81 et seq. FMIA.

582 Art. 4 FMIA.

In post-trading via a blockchain or DLT infrastructure, the function of central counterparty does not exist. Counterpositions of different trading participants are not netted prior to settlement in the securities settlement and depository system. Instead, settlement takes place continually on a gross basis.[583]

By interposing between the buyer and the seller, the central counterparty also assumes the counterparty default risks in securities and derivatives trading. This function does not exist on the blockchain environment either, so the existing counterparty risk for trading participants in securities and in particular in derivatives trading could rise. In many cases, this risk will not be significant, because the trading participants only handle limited volumes in view of their presumably small size and because settlement is carried out automatically and promptly via smart contracts.

Given this background, amendments to regulations on central counterparties to take account of blockchain-/DLT-based models do not currently seem necessary.

c) Central securities depositories / securities settlement systems

In accordance with FMIA, the operator of a central custodian or securities settlement system is considered to be a central securities depository. A central custodian is an entity for the central custody of securities and other financial instruments based on uniform rules and procedures. A securities settlement system is an entity for the clearing and settlement of transactions in securities and other financial instruments based on uniform rules and procedures.[584]

The current provisions on central custodians and securities settlement systems were not drafted to take account of blockchain- and DLT-based systems. Accordingly, it is, for example, not sufficiently clear whether and to what extent the settlement activity of blockchain-based platforms is in line with the applicable provisions in FMIA on post-trading. In view of the broad, technology-neutral legal definition, it is conceivable that blockchain-based concepts can also be classified as securities settlement systems within the meaning of FMIA. For example, it could be argued that in the clearing and safekeeping of tokens with the characteristics of securities via smart contracts, transactions are cleared and settled based on "uniform rules and procedures", and hence the activity is that of a central securities depository subject to authorisation. In accordance with prevailing provisions, such a central securities depository would have to be operated by another legal entity than the trading venue and be authorised separately.[585]

The introduction of a central securities depository in a generally decentralised concept such as blockchain or DLT seems initially to run counter to the system. At the same time, it may be necessary, e.g. for the purpose of system protection, to introduce the function of a central securities depository into such a system.

Any requirement for authorisation as a central securities depository (e.g. for a token-based securities settlement system) would present a high barrier to market entry, however. The introduction of a minimum volume for the authorisation requirement for central securities depositories (i.e. for central custodians and securities settlement systems) would be a pragmatic solution with respect to blockchain and DLT systems as well as system protection. Another solution, which is suggested below, is to create a new authorisation category in

---

583 This does not apply, for example, in the case of derivatives with a certain duration. In this context, it must be noted that a clearing duty applies for certain derivative transactions. If trading venues accept trading of such specified derivatives subject to a clearing duty, a blockchain-based trading venue must also enable a connection to a central counterparty in order to prevent regulatory arbitrage.

584 Art. 61 FMIA.

585 Art. 10 FMIA.

financial market infrastructure law, which entails a combination of trading and post-trading functions (e.g. securities settlement).[586]

Moreover, in the light of the observable integration of trading and post-trading infrastructures specifically in the context of blockchain and DLT, the requirement that a legal entity can only operate one financial market infrastructure[587] should be critically examined and a more flexible approach defined – provided that this makes sense and is acceptable from a risk point of view.[588] In this context, the additional legal requirements in the area of post-trading and the delimitation of activities in the various financial market infrastructures (e.g. when can a securities settlement system be deemed a central securities depository?) must be clarified in greater detail following publication of this report.

6.4.7 Innovation areas in financial market infrastructure law and the creation of a new authorisation category

6.4.7.1 Innovation areas (sandboxes) in financial market infrastructure law

In financial market infrastructure law, there is currently no innovation area comparable to that in banking law[589]. Compared with bank authorisation, however, the applicable requirements in financial market infrastructure law present lower barriers to market entry. Additionally, these requirements often do not present a direct barrier to market entry, but rather have an indirect effect. For example, the classification of a token as a security entails relative low costs for the business model underlying the token. However, classification as a security has a greater impact on secondary trading (e.g. the classification as a security can result in the need for trading venue authorisation).

In banking law, an innovation area (sandbox) of up to CHF 1 million currently applies. Nonetheless, "small-scale" business models are generally not tested in the specific case of ICOs. Instead, project financing is sought via ICOs for substantial amounts in some instances. A sandbox in financial market infrastructure law would therefore have to have high limits (namely a substantially higher limit than is currently the case in banking law), which would lead to additional risks in the area of investor protection.

As well as ensuring the proper functioning and transparency of the securities and derivatives markets and the stability of the financial system, the focus with blockchain- and DLT-based business models in particular is on protecting financial market participants and treating investors equally. A regulatory carve-out – i.e. with a comprehensive exemption for blockchain projects from all requirements in financial market infrastructure law – would ostensibly help to provide innovation-friendly framework conditions. At the same time, the interests of financial market participants and investors would be placed last, and treatment would be unequal compared with non-blockchain securities and derivatives.

Instead, it should be examined which provisions in financial market infrastructure law for blockchain- and DLT-based business models could lead to specific challenges. As indicated[590], such challenges exist namely in the areas of trading tokens via central trading platforms and in the application of financial market law to decentralised financial market "infrastructures". The attractiveness of Switzerland for blockchain and DLT projects depends on the provision of a targeted, appropriate financial market regulatory framework for such projects. Hence, it seems more expedient to address the challenges in financial market infrastructure law that are specific

586 See section 6.4.7.2.
587 See Art. 10 FMIA.
588 See section 6.4.3 at the end.
589 See section 6.3.2.
590 See section 6.4.4.

to blockchain/DLT applications by means of specific amendments (instead of a regulatory carve-out).[591]

6.4.7.2 Creation of a new authorisation category for financial market infrastructures in the blockchain/DLT area

For the above reasons, the Federal Council proposes creating a new authorisation category for a financial market infrastructure type involving crypto-based assets by amending FMIA and FMIO with the following key points:

- *Authorisation category specifically for blockchain and DLT*

  The aim of the new financial market infrastructure category is to create a legal framework for the new forms of infrastructure possible in view of technological developments and to take full account of the current legal purpose of FMIA at the same time. By way of a partial derogation and exemption from the technology-neutral approach, a technology-specific authorisation category geared to blockchain and DLT applications in the area of finance is proposed, which still takes up the protective aims of FMIA and applies them to blockchain/DLT technology.

- *Basic features of the new authorisation category*

  In terms of content, the new authorisation type is based on the points set out above.[592] Both retail participants and regulated participants should be able to participate in the new infrastructure and trade in tokens. Trade with tokens should be able to operate multilaterally and in accordance with non-discretionary rules, and should encompass both securities tokens and non-securities tokens. Additionally, all processes should be able to run digitally.

  The currently applicable duties in securities trading (e.g. in the areas of market transparency and integrity, investor protection, combating money laundering and terrorist financing, etc.) would remain unchanged in terms of content. Some of these duties would have to be linked to the operation of the infrastructure, however, and thus to the holder of authorisation, partly because the new authorisation category is intended to permit non-intermediated trading with securities tokens, without the involvement of the securities dealer, for example.

- *Holistic regulation of blockchain financial market infrastructure instead of differentiation*

  In the "traditional" world of central financial market infrastructures, there is a clear differentiation between infrastructure for trading (e.g. stock exchanges) and in the area of post-trading (e.g. central securities depositories, securities settlement systems). The aim is to prevent the destabilisation of one financial market infrastructure from spreading vertically to another financial market infrastructure and to preclude the emergence of misplaced incentives. In the area of blockchain/DLT, trading and settlement of a financial transaction can take place practically at the same time, making this kind of delimitation impractical. Against this backdrop, the new financial market infrastructure category should comprise one single authorisation holder, encompassing not just trade with tokens but also post-trading activities.

- *Regulatory implementation*

  The principles of the new authorisation (such as requirements of the organisation, fit and proper requirements, capital requirements, etc.) would be anchored in the law (FMIA) and implemented by the Federal Council in the corresponding ordinance

591 See section 6.4.7.2.
592 See section 6.4.4.

(FMIO). To take account of rapid technological developments, FINMA should be given the power – in a framework that is clearly defined in the respective law and ordinance – to make specific requirements of such authorisation holders in a practical, individual form. The aim is to be able to take account of the specific services of an authorisation holder.

6.4.7.3 Outlook: regulation of decentralised financial market "infrastructures"

In practice – today at least – there are a large number of centrally organised financial market infrastructures in the blockchain world too (e.g. crypto exchanges, wallet providers and others). These providers are often the link between the traditional, centralised financial world and the new decentralised blockchain and DLT models. At the same time, it seems that infrastructure services – such as trade with tokens – might become increasingly decentralised, but it is too early to tell definitively.

This paradigm shift (i.e. the shift from centralised to decentralised structures) also poses major challenges for the regulator. It can be generally assumed that the same aims will apply in decentralised structures as in centrally organised financial markets and infrastructures: ensuring the proper functioning and transparency of the financial markets and the stability of the financial system, as well as protecting financial market participants and treating investors equally. Nonetheless, there are a number of questions on how these aims can be achieved in a decentralised environment. With respect to the increasing decentralisation, for example, it can be seen that financial market regulations that focus on the operators of an infrastructure (an entity-based approach) will increasingly face specific challenges in future. Alternatively, regulations could concentrate more on specific activities (activity-based approach) and thus be geared to both central and decentralised financial market infrastructures.

It seems clear that further conceptual development of regulatory approaches and instruments is necessary in view of the paradigm shift from central to decentralised financial markets and infrastructures triggered by blockchain and DLT models. However, it is neither clear today nor is it possible to foresee what form regulation of decentralised financial market infrastructures (or decentrally organised financial markets) should ultimately take. The Federal Council will continue to observe these developments accordingly and present a practical regulation proposal on decentralised financial market infrastructures in due course.

6.4.8 Market conduct rules in securities and derivatives trading

6.4.8.1 General

In addition to regulatory provisions on financial market infrastructures, FMIA also contains rules on derivatives trading[593], as well as the provisions on the disclosure of shareholdings[594], public takeover offers[595] and insider trading and market manipulation[596] (market conduct rules).

593 Art. 93 et seq. FMIA.
594 Art. 120 et seq. FMIA.
595 Art. 125 et seq. FMIA.
596 Art. 142 et seq. FMIA.

6.4.8.2 Trade with derivatives

FMIA sets out provisions on trading in derivatives that correspond to international standards. The provisions contain a clearing duty[597], a reporting duty[598], risk mitigation duties[599] and a platform trading duty[600].[601]

- *Clearing duty*: In accordance with Article 97 et seq. FMIA, standardised OTC derivatives must be cleared via central counterparties. Article 101 FMIA gives FINMA the power to determine the derivatives to which this duty applies. The scope of this clearing duty is limited to large financial or non-financial counterparties[602].
- *Reporting duty*: In accordance with Article 104 et seq. FMIA, derivatives transactions must be reported to a trade repository authorised or recognised by FINMA. Both financial and non-financial counterparties are subject to this reporting duty.
- *Risk mitigation duties*: Article 107 FMIA sets out risk mitigation duties for OTC derivatives that are not cleared via a central counterparty.
- *Platform trading duty*: In Article 112 et seq. FMIA, the legal basis was created to require large financial and non-financial counterparties to trade derivatives classified by FINMA as standardised via an authorised or recognised trading venue or via an authorised or recognised operator of an organised trading system. The corresponding provisions entered into force on 1 August 2017. FINMA has not yet made any derivatives subject to a platform trading duty[603].

One of the main goals of duties in connection with the trade in (OTC) derivatives is to minimise systemic risks.

As mentioned before[604], the derivative trading rules were not drafted to take account of novel derivatives in the form of tokens either inside or outside Switzerland, but instead are intended to regulate traditional OTC derivatives. Moreover, FMIA does not explicitly answer the question of whether derivative trading duties are applicable to tokens that have the form of derivatives. In any case, it is clear that at present they are not subject to either a clearing duty or a trading duty. Such derivatives are as yet insignificant in Switzerland. Should this change in future, it must be checked to what extent derivative trading duties can be implemented for derivatives in the form of tokens.

6.4.8.3 Disclosure of shareholdings

Like the provisions on insider trading and market manipulation, the provisions on the disclosure of shareholdings and on public takeover offers have been taken over in FMIA unchanged from SESTA and apply to all financial market participants.[605] It is currently thought that the reporting duty within the meaning of Article 120 FMIA applies also to tokens that can be considered to be shares or derivative holdings subject to reporting.

6.4.8.4 Public takeover offers

Anyone who directly, indirectly or acting in concert with third parties acquires equity securities which, added to the equity securities already owned, exceed the threshold of 33⅓% of the

---

597 Art. 97 et seq. FMIA.
598 Art. 104 et seq. FMIA.
599 Art. 107 et seq. FMIA.
600 Art. 112 et seq. FMIA.
601 See Dispatch regarding FMIA, 7499.
602 Art. 98 FMIA and Art. 99 FMIA; for the definition of financial counterparty, see Art. 93 para. 2 FMIA.
603 FINMA determines which derivatives are subject to a platform trading duty (see Art. 113 FMIA).
604 See section 6.4.2.3.
605 Dispatch regarding FMIA, 7500.

voting rights of a target company, whether exercisable or not, must make an offer to acquire all listed equity securities of the company. Target companies may raise this threshold to 49% of voting rights in their articles of incorporation.[606]

Equity securities are considered to be shares, participation certificates, profit-sharing certificates or other participation rights.[607] Target companies are companies with their registered office in Switzerland whose equity securities are at least partly listed on a stock exchange in Switzerland or companies with their registered office abroad that have the main listing of at least some of their equity securities in Switzerland.[608] The main purpose of the duty to make an offer is to protect minority shareholders from a change of control of the company that would be disadvantageous to them.[609]

From the current perspective, the provisions on public takeover offers also apply to tokens representing equity securities that are subject to the provisions on public takeover offers.

6.4.8.5 Insider trading and market manipulation

Article 142 paragraph 1 FMIA and Article 143 paragraph 1 FMIA contain regulatory bans on insider trading and market manipulation, which apply to all market participants.[610]

In accordance with Article 142 paragraph 1 FMIA, any person who has insider information and who knows or should know that it is insider information or who has a recommendation that he or she knows or should know is based on insider information behaves inadmissibly if he or she exploits it to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use financial instruments derived from such securities, discloses it to another or exploits it to recommend to another to acquire or dispose of securities admitted to trading on a trading venue in Switzerland or to use financial instruments derived from such securities.

In accordance with Article 143 paragraph 1 FMIA, a person behaves inadmissibly if he or she publicly disseminates information which he or she knows or should know gives false or misleading signals regarding the supply, demand or price of securities admitted to trading on a trading venue in Switzerland or carries out transactions or acquisition or disposal orders which he or she knows or should know give false or misleading signals regarding the supply, demand or price of securities admitted to trading on a trading venue in Switzerland.

Based on the above, the regulatory offences of both insider dealing and market manipulation must involve securities that are admitted for trading on a stock exchange or multilateral trading facility in Switzerland. This also applies to tokens that take the form of securities. Other securities or tokens are not comprised and are thus treated equally. There is therefore no specific need for action with respect to tokens at present.

6.4.9 Conclusion

In the opinion of the Federal Council, it is not necessary to use legal amendments to prevent tokens from being deemed securities or derivatives. Instead, it makes more sense to ensure that the provisions applicable to securities and derivatives can be meaningfully applied to tokens so that they will be regulated efficiently. Accordingly, the focus must be placed on the legal consequences of classifying tokens as securities and derivatives. The Federal Council therefore proposes the following measures in financial market infrastructure law:

606 Art. 135 para. 1 FMIA.
607 Art. 2 let. i FMIA.
608 Art. 125 FMIA.
609 See in particular Barthold/Schilter 2017: Art. 135 FMIA no. 6 et seq.
610 See on insider trading and price manipulation, Art. 154 FMIA and Art. 155 FMIA.

- Creating a new authorisation category for providers of financial market infrastructures in the blockchain/DLT area by means of an addition to FMIA and FMIO;[611]
- Making it possible for market participants to apply for authorisation, even if solely for the purpose of operating an OTF;[612]
- Making regulations on ancillary services of financial market infrastructures more flexible by amending FMIA and FMIO;[613]
- Creating additional legal certainty on the question of whether derivative trading duties also apply to derivatives in the form of tokens. From the current perspective, there is no need for action with respect to the other market conduct rules.[614]

6.5 Financial Institutions Act (FinIA)

6.5.1 Introduction

The new Financial Institutions Act (FinIA; SR *954.1*) sets out the requirements applicable to the activities of financial institutions, that is, portfolio managers, managers of collective investments, fund management companies and securities firms. The question can be asked as to what extent FinIA is applicable to blockchain- and DLT-based business models and whether this is appropriate. It must primarily be clarified whether the issue of tokens or trade with tokens requires an authorisation as a securities firm. Token management services are ultimately conceivable, which raises the question of whether an authorisation as a portfolio manager is required.[615]

6.5.2 Legal situation in accordance with FinIA

6.5.2.1 Legal basis

General

On 15 June 2018, Parliament adopted the Financial Institutions Act (FinIA) together with the Financial Services Act (FinSA). FinIA sets out a consistent supervisory regime for financial institutions (portfolio managers, managers of collective investments, fund management companies and securities firms). A new key element is that portfolio managers of individual client assets, managers of pension fund assets and trustees are now subject to prudential supervision. FinIA is set to enter into force on 1 January 2020 together with FinSA.

Portfolio managers

Anyone who, in line with a mandate, is able to dispose professionally of client assets in the name and for the account of said client in accordance with Article 3 letter c numbers 1–4 FinSA is considered to be a portfolio manager[616] and needs authorisation from FINMA[617] and must be affiliated to a supervisory body.

An independent economic activity aimed at realising earnings in the long-term is considered to be professional.[618] The term is to be clarified in the Ordinance to the Financial Institutions

611 See section 6.4.7.2.
612 See section 6.4.4.2.
613 See section 6.4.3.
614 See section 6.4.8.
615 See section 6.7. regarding classification as a portfolio manager of collective investment schemes.
616 Art. 17 para. 1 FinIA
617 Art. 5 para. 1 FinIA
618 Art. 3 FinIA

Act (FinIO) currently in consultation. Hence, portfolio managers (and trustees) are acting professionally, if:[619]

- they earn gross income of more than CHF 50,000 per calendar year,
- they take up business relationships with more than 20 contractual parties per calendar year that are not linked to one-time activity or maintain at least 20 such relationships per calendar year,
- they have permanent power of disposal over third-party assets that exceed CHF 5 million at any point in time, or
- they carry out transactions whose total volume exceeds CHF 2 million per calendar year.

The term "asset" is not explicitly defined in FinIA. Based on the text of the dispatch[620], it can be assumed that it encompasses not just the financial instruments defined in FinSA – in particular equity securities, debt instruments, units in collective investment schemes, structured products and derivatives[621] – but also all other financial investments, such as sight or time deposits and debt instruments without the character of securities. This may also include tokens if they are classified as securities or constitute another financial asset.

Portfolio managers – together with trustees – are in the lowest position in the authorisation hierarchy for portfolio management introduced with FinIA. This means that authorisation as a portfolio manager does not entitle the authorisation holder to carry out any other activity that needs authorisation.[622] Accordingly, the legal requirements of the activity of portfolio managers are lower than for other financial institutions with higher forms of authorisation (managers of collective investments, fund management companies, securities firms).

Securities firm

In this context, the provisions in FinIA on the activity of a securities firm are of primary interest, next to the provisions on the activity of a portfolio manager. The provisions on securities firms essentially correspond to the current provisions on securities dealers in the SESTA.[623] In accordance with these provisions, any party that trades with securities professionally in its own name for the account of clients is to be considered a securities firm and needs FINMA authorisation.[624] Own-account dealers and market makers are also deemed to be securities firms.[625]

The term "security" is defined in Article 3 letter b FinSA. For further details, see section 6.4.2. As mentioned above, an independent economic activity aimed at realising earnings in the long-term is considered to be professional.[626] The term is to be clarified in the draft FinIO. In accordance with the relevant provisions[627], an activity is considered professional if accounts are managed for more than 20 clients or securities are held in custody for more than 20 clients.[628] Hence, the current legal situation will continue to apply.[629]

---

619 Art. 11 V-FinIO
620 Dispatch regarding FinSA/FinIA, 8943.
621 See Art. 3 let. a FinSA.
622 See Art. 6 FinIA.
623 See Art. 41 et seq. FinIA.
624 See Art. 5 para. 1 in conjunction with Art. 41 let. a FinIA.
625 See details in Art. 41 let. b and c FinIA.
626 Art. 3 FinIA.
627 Art. 57 para. 1 E-FinIO.
628 See Art. 57 para. 1 E-FinIO.
629 See FDF Explanatory report FinSO/FinIO 2018: 97.

Article 12 FinIA should also be noted. It stipulates that authorisation as a securities firm or bank is necessary for persons that professionally underwrite securities issued by third parties and offer them to the public in the primary market ("issuing houses") or that professionally create derivatives in the form of securities and offer them to the public in the primary market ("derivative firm").

In the new authorisation hierarchy introduced in FinIA, securities firms are between banks and managers of collective assets.[630] Accordingly, the legal requirements for exercising the activities of a securities firm – for example with respect to minimum capital – are less strict than for a bank, but stricter than for a manager of collective investments.

6.5.2.2 Management of tokens

The question of whether token management constitutes an activity subject to authorisation within the meaning of FinIA depends on the individual case. If it can be deemed to be portfolio management within the meaning of the law,[631] it must be clarified whether the activity is being exercised professionally. The conditions for an activity to be considered professional are not very stringent, which means that this criterion will likely be met on a frequent basis. If the activity is considered to be portfolio management within the meaning of FinIA, the persons in question must obtain corresponding FINMA authorisation and become affiliated to a supervisory body.

6.5.2.3 Issue of tokens

The creation of tokens as an own issue does not require (securities firm) authorisation, even if the said tokens have the characteristics of securities. The same applies to the public offering of securities. By contrast, any person that professionally creates derivatives in the form of securities and offers them to the public in the primary market ("derivative firm") requires authorisation as a securities firm – or as a bank. It must be determined on a case-by-case basis whether tokens are to be classified as derivatives in the form of securities. With respect to the activity of a derivative firm, it must still be clarified in the drafting of FinIO whether the term "professional" is to be defined in the same way as in Article 57 E-FinIO.

As indicated, a person that professionally underwrites securities issued by third parties and offers them to the public in the primary market also needs authorisation as a bank or securities firm. This also applies to the issue of tokens that can be classified as securities.

6.5.2.4 Professional trading with tokens

Any person that trades professionally in its own name for the account of clients with tokens that can be classified as securities also needs authorisation as a securities firm. Pure custody of such tokens, the return of tokens from the custodian to the client or the transfer of tokens by the custodian to a third party in the name of the client does not constitute trading. As indicated, activity is considered professional if accounts are managed for more than 20 clients or securities are held in custody for more than 20 clients.[632]

6.5.3 Conclusion

There are currently no specific barriers to market entry or any regulatory loopholes for blockchain- and DLT-based business models with respect to obtaining authorisation as a portfolio manager. Consequently, there is no need for regulatory action. The corresponding requirements for authorisation and operation are fairly undemanding and, if the parties in

630 See Art. 6 FinIA.
631 See regarding definition Art. 17 para. 1 FinIA and section 6.5.2.1.
632 See Art. 57 para. 1 E-FinIO; on the need for professionalism in accordance with applicable law, see FINMA Circ. 2008/5: margin no. 11 et seq.

question also manage conventional assets, they need authorisation as a portfolio manager anyway.

The record-keeping and reporting duties applicable to securities firms are discussed in section 6.4.4. With respect to the proposal that authorisation may be requested solely for the purpose of operating an OTF, see the relevant remarks concerning FMIA.[633]

6.6 Federal Financial Services Act (FinSA)

6.6.1 Introduction

The new Federal Financial Services Act (FinSA)[634] aims to guarantee client protection in the financial services sector and create comparable conditions for the provision of financial services by financial service providers. There are thus points of reference to players in the area of crypto-based assets and blockchain applications[635] and their clients. It must be clarified to what extent these participants and their services are subject to FinSA and whether there is a need for legal amendments to protect clients or because of requirements that are inappropriate for providers of tokens and blockchain-based services.

6.6.2 Legal bases

6.6.2.1 Purpose and scope of FinSA

FinSA aims to protect clients and create comparable conditions for the provision of financial services by financial service providers. Clients are all considered to be creditors and investors to whom a financial service provider provides a service.[636] The provisions in FinSA aim to improve transparency as well as setting out clear requirements of service providers' conduct in order to create the conditions for clients to be able to take independent decisions regarding the investment of their assets.[637]

The scope of the law in accordance with Article 2 FinSA encompasses financial service providers, client advisors and the issuers and providers of financial instruments. The financial market laws, especially the new FinIA[638], should be consulted regarding the supervision of financial service providers, issuers of financial instruments and providers of financial instruments.[639] FinSA does not set out any new prudential standards for these institutions, but clarifies certain specific organisational requirements with respect to implementation of conduct rules.[640] The aim is to regulate conduct and the duty to provide information at points of sale.[641]

6.6.2.2 Financial instruments and securities in accordance with FinSA

Article 3 letter a FinSA defines the financial instruments that come under the scope of FinSA. In accordance with Article 3 letter a number 1-2 FinSA, securities that constitute equity securities or debt instruments are deemed to be financial instruments. The term "equity

633 See section 6.4.
634 SR **950.1**; adopted by the Federal Assembly on 15 June 2018, entry into force planned for start of 2020.
635 See section 2.4.
636 Dispatch regarding FinSA/FinIA, 8940
637 Dispatch regarding FinSA/FinIA, 8940
638 SR **954.1**
639 See section 6.5.
640 Art. 21–27 FinSA; see also Dispatch regarding FinSA/FinIA, 8942.
641 Dispatch regarding FinSA/FinIA, 8921: "The regulatory provisions on conduct in FinSA do not intervene directly in the relationship under private law between financial service providers and clients. Hence, they are not mixed-law provisions, but public-law provisions. The civil judge will continue to judge the civil-law relationship based on provisions under private law. To clarify these provisions, however, the civil judge may refer to the regulatory provisions on conduct in FinSA".

security" refers to securities that grant participation and voting rights in corporations. This encompasses shares in their various forms[642], participation and dividend-right certificates[643], including share-like securities that grant participation and voting rights, as well as securities such as convertible bonds that contain the right to purchase shares or share-like securities.[644] The term "debt instrument" refers to securities that are not classified as equity securities, in particular bonds, derivatives and structured products[645]. It can be seen from the Federal Council dispatch on FinSA and FinIA that the chosen definition in Article 3 letter a number 1 and 2 is intended to include various forms of securities. In accordance with Article 3 letter b number 6 FinSA, financial instruments also include deposits whose repayment value or interest is dependent on risk or on market prices, except for those whose interest rate is linked to an interest rate index.

The term "securities" in Article 3 letter b FinSA is identical to the term "securities" in FMIA and thus comprises certificated and uncertificated securities, derivatives, and intermediated securities that are standardised and suitable for mass trading[646].

In accordance with the remarks in section 5.1, uncertificated securities may be created in the context of ICOs. If such tokens are offered publicly in the same structure and denomination or placed with more than 20 clients (and if they are not created specifically for individual counterparties), they constitute securities within the meaning of FinSA. The decision to classify a token as a financial instrument in accordance with FinSA depends on the token's economic function and hence on the right that it secures. This decision must be made on a case-by-case basis in view of the wide range of forms that tokens can take. The crucial criterion for classifying a token as a financial instrument within the meaning of Article 3 letter a numbers 1 and 2 FinSA is whether acquisition of the token grants the holder participation rights, voting rights or rights to the repayment of debt, as indicated above.

Payment tokens are not securities and therefore are not financial instruments within the meaning of FinSA. The same applies for utility tokens, which are intended to provide access to a digital function or service. Nonetheless, payment tokens can be financial instruments under the conditions of Article 3 letter a number 6 FinSA if they are accepted as deposits.[647]

By contrast, classification as a financial instrument is not of key relevance, at least for the duties of the issuer of the (securities) token in accordance with FinSA, as the prospectus requirements apply in any case if securities – and not financial instruments – are offered publicly.[648] For tokens that are securities[649], the prospectus requirements apply as a minimum, provided that the other conditions are fulfilled (for example in case of a public offering).[650]

6.6.2.3 Financial services and financial service providers in accordance with FinSA

The term "financial services" in accordance with Article 3 letter c FinSA is deliberately defined generally, as FinSA contains cross-sector regulations. It regulates all activities that can lead to the acquisition of a financial instrument by a client. This includes the acquisition and sale of financial instruments for the account of clients, irrespective of whether the financial instruments are acquired by third parties or issued, placed or sold in the secondary market by the financial service providers themselves (number 1). Mere brokering of transactions in financial

642 Art. 622 CO.
643 Art. 656a and 657 CO.
644 Dispatch regarding FinSA/FinIA, 8943
645 Dispatch regarding FinSA/FinIA, 8943
646 See section 6.4.
647 See section 6.2.
648 See section 6.6.5.1.
649 See section 5.1.
650 See section 6.6.4.3.

instruments (number 2), as well as portfolio management and investment advice are also considered to be financial services. Portfolio management is deemed to comprise all activities for which the financial service provider is given power of attorney to invest assets for the account of the clients (number 3). By contrast, if the financial service provider recommends the purchase or sale of financial instruments to specific clients, this constitutes investment advice.[651]

Financial service providers in accordance with Article 3 letter d FinSA are any persons that provide financial services on a professional basis in accordance with Article 3 letter c FinSA in Switzerland or for clients in Switzerland. This captures supervised market participants, such as banks, securities firms, fund management companies and now also all portfolio managers.[652] The institutions in question must ensure that their employees and third parties that they use to provide financial services comply with the conduct rules. Furthermore, non-supervised market participants are also subject to the conduct rules if they provide financial services to their clients. No monitoring is carried out of such market participants' compliance with the conduct rules, but violations are subject to criminal penalties.[653]

If financial service providers exercise an independent economic activity aimed at realising earnings in the long-term within the meaning of Article 2 letter b of the Commercial Register Ordinance of 17 October 2007 (CRO)[654], this is deemed to be professional activity. An activity is assumed to be professional if the financial service provider supplies financial services for more than 20 clients or advertises the provision of financial services in advertisements, prospectuses, circulars or electronic media.[655]

6.6.3 Players in the crypto area and FinSA

This section examines various players in the crypto area[656] to determine whether they are financial service providers in accordance with FinSA and thus provide financial services within the meaning of FinSA.

Mining

Mining of tokens in itself does not constitute a financial service within the meaning of Article 3 letter c FinSA. It does not fulfil the requirement of an activity performed for clients with respect to the acquisition or the sale of financial instruments or the acceptance and brokering of orders involving financial instruments, at least in cases in which the mined tokens do not constitute financial instruments in accordance with FinSA.[657] If, for example, tokens are mined that have the sole function of a cryptocurrency, the miner is not a financial service provider in accordance with Article 3 letter d FinSA.

By contrast, if tokens are mined that constitute financial instruments within the meaning of FinSA, the classification of a miner as a financial service provider depends above all on how close and concrete the client relationship is in terms of a contractual relationship (mandate). The mandate must focus in practical terms on the purchase or sale of financial instruments or the acceptance and brokering of orders that involve financial instruments.

---

651 See regarding the entire paragraph Dispatch regarding FinSA/FinIA, 8946-8947.
652 Art. 3 let. d FinSA.
653 See Art. 89 et seq. FinSA.
654 SR **221.411**
655 Dispatch regarding FinSA/FinIA, 8947. This is based on the previous regulations in BankA.
656 See section 2.4.
657 See section 6.6.2.2.

Wallet app developers

The development of software that allows users to manage their tokens does not constitute a financial service within the meaning of Article 3 letter c FinSA, even if the tokens are financial instruments within the meaning of Article 3 letter a FinSA. It does not fulfil the requirement of an activity performed for clients with respect to the purchase or the sale of financial instruments or the acceptance and brokering of orders involving financial instruments. Hence, a pure wallet app developer is not a financial service provider and is not required to observe the duties set out in FinSA. This seems appropriate and unproblematic with respect to client protection, given that comparable software providers in the traditional financial world do not come under the scope of FinSA.

Crypto trading platforms

Crypto trading platforms or crypto exchanges allow clients to buy and sell tokens directly (i.e. without the involvement of an intermediary). They may take various technical forms.[658] If retail clients can purchase tokens via a crypto exchange from its holdings without pure matching, and these tokens are financial instruments in accordance with FinSA, the operator is generally considered to be a financial service provider within the meaning of Article 3 letter d FinSA. In such constellations, the operator is offering its clients financial services, such as transactions aiming to purchase or sell financial instruments.[659] Accordingly, they are subject to the conduct rules in Article 7–20 FinSA, especially the duty to provide information in accordance with Article 8 FinSA and the documentation and accountability duties in Article 15 and 16 FinSA. The possible exceptions should be noted, which apply if client orders are only executed or forwarded, that is, no advisory services or similar are provided (so-called execution-only transactions). In such cases, the financial service provider is exempt, for example from the duty to supply a key information document[660] and from the duty to check the suitability and appropriateness.[661]

Custody services

The custody of assets, be it tokens or assets in the analogue world, does not in itself constitute a financial service within the meaning of Article 3 letter c FinSA, even if the tokens are financial instruments within the meaning of Article 3 letter a FinSA. It does not fulfil the requirement of an activity performed for clients with respect to the purchase or the sale of financial instruments or the acceptance and brokering of orders involving financial instruments. Portfolio management in accordance with FinSA is deemed to comprise all activities for which the financial service provider is given power of attorney to invest assets for the account of its clients. On the other hand, if the sole purpose of the asset transfer is for safe custody and there is no power of attorney to invest the assets, the activity does not comprise portfolio management.

Accordingly, FinSA does not apply to providers of custody services, provided that their service is restricted exclusively to custody.

On the other hand, if the sale of tokens that are classified as financial instruments is only possible via an account at the provider of custody services, for example, because the private key is located there, the activity constitutes a financial service in accordance with Article 3 letter c number 1 or 2 FinSA. Providers of such custody services are therefore financial service providers in accordance with Article 3 letter d FinSA and are subject to the conduct rules in

658 Art. 2.4.
659 Art. 3 let. c no. 1 and 2 FinSA.
660 Art. 8 para. 4 FinSA.
661 Art. 13 para. 1 FinSA.

Article 7–20 FinSA, especially the duty to provide information in accordance with Article 8 FinSA and the documentation and accountability duties in Article 15 and 16 FinSA. The possible exceptions should be noted, which apply if client orders are only executed or forwarded, that is, no advisory services or similar are provided (execution-only transactions). In such cases, the financial service provider is exempt, for example from the duty to supply a key information document[662] and from the duty to check the suitability and appropriateness.[663]

Crypto brokerage

Companies that purchase or sell tokens in the secondary market on behalf of clients meet the conditions to be deemed financial service providers in accordance with Article 3 letter c in conjunction with Article 3 letter d FinSA, provided that the tokens can be classified as financial instruments within the meaning of Article 3 letter a FinSA.[664] The conditions are met in this case because the activity in question aims to purchase or sell financial instruments for clients or because orders are accepted and forwarded that involve financial instruments.[665] If these services are provided professionally by companies in Switzerland or for clients in Switzerland, the crypto brokers in question are financial service providers in accordance with Article 3 letter d FinSA.

As a result, they are required to comply with the FinSA conduct rules. Accordingly, crypto brokers must divide their clients into segments in accordance with Article 4 FinSA. Additionally, they are subject to the duty to provide information in accordance with Article 8 FinSA. They are also required to check appropriateness and suitability in accordance with Article 11 and 12 FinSA. The possible exceptions should be noted, which apply if client orders are only executed or forwarded, that is, no advisory services or similar are provided (execution-only transactions). In such cases, the financial service provider is exempt, for example from the duty to supply a key information document[666] and from the duty to check the suitability and appropriateness.[667]

The Federal Council considers it appropriate that crypto brokers should be subject to the same code of conduct as brokers of traditional financial instruments. In the case of investments in tokens classified as financial instruments, appropriate client protection seems particularly important in view of the novel nature and risks of such financial instruments.

Other service providers

Service providers that facilitate or settle pure payment services by means of tokens do not come under the scope of FinSA. The same applies for other service providers that facilitate payment transactions with conventional currencies in the analogue world (for example credit card providers). The financial instrument requirement, at least, is not met here: payment tokens and also conventional currencies do not constitute financial instruments within the meaning of Article 3 letters a and b FinSA.

On the other hand, traditional service providers, such as banks and portfolio managers, that buy tokens in the secondary market or recommend such a purchase for clients in the context of a portfolio management agreement or investment advice, can normally be considered to be financial service providers in accordance with FinSA, provided that the tokens in question can be classified as financial instruments within the meaning of Article 3 letter a.[668] The conduct rules in Articles 7–20 FinSA therefore apply to these service providers in the same way as it

662 Art. 8 para. 4 FinSA.
663 Art. 13 para. 1 FinSA.
664 See section 6.6.2.2.
665 Art. 3 let. c no. 1 and 2 FinSA.
666 Art. 8 para. 4 FinSA.
667 Art. 13 para. 1 FinSA.
668 See section 6.6.2.2.

applies to traditional financial instruments. There is no differentiation between the analogue and the digital world in such activities. Such equal treatment is fundamentally appropriate.

6.6.4 ICOs from the FinSA perspective

To determine the relevance of FinSA for ICOs, it must be clarified whether the token issuer is a financial service provider and the issue of tokens a financial service in accordance with FinSA or whether the issuer of tokens is an issuer and/or producer in accordance with FinSA, and whether the prospectus requirement applies in case of a public offering. Remarks on the classification of tokens as securities and financial instruments within the meaning of FinSA are set out in section 6.6.2.2.

6.6.4.1 Initial issue of tokens as a financial service?

The initial issue of tokens in an ICO in the primary market does not fit the definition of a financial service in FinSA, because it does not meet the condition of being an activity provided for the client, which is generally based on a contract or a contract-like relationship between the financial service provider and clients. By contrast, sales of tokens by the company to third parties are not made for the account of these purchasers, but directly to the third parties, or possibly to financial intermediaries, which in turn act for the account of third parties. The initial issue itself in the form of an ICO and the prior production of the token are not financial services within the meaning of FinSA either, which means that the duty to inform and the code of conduct do not apply. On the other hand, other duties in FinSA do apply.[669]

As the initial issue of tokens in an ICO is not a financial service within the meaning of FinSA, the company that issues the tokens is not a financial service provider in accordance with FinSA. Moreover, any company that issues tokens once only is unlikely to meet the requirement for professional activity with respect to the provision of financial services, which would be a condition for classification as a financial service provider. In any case, the one-time issue of tokens in the primary market should not be classified as an independent economic activity aimed at realising earnings in the long-term in the context of providing financial services.

6.6.4.2 Issuer and producer in an ICO

In accordance with Article 3 letter f FinSA, an issuer is a person who issues securities or arranges for securities to be issued for the purpose of obtaining capital.[670] Persons that issue a financial instrument or that make changes to an existing financial instrument – for example to its risk/return profile – are producers within the meaning of Article 3 letter i FinSA.

Companies that issue tokens as part of an ICO that can be classified as securities[671] are therefore issuers within the meaning of Article 3 letter f FinSA and must therefore comply with the duty to publish a prospectus in accordance with Article 35 et seq. FinSA[672]. If these tokens are classified as financial instruments in accordance with Article 3 letter a FinSA[673], the company is also a producer within the meaning of Article 3 letter i FinSA. Producers of financial instruments must draw up a key information document,[674] unless they are exempt in accordance with Article 59 FinSA.[675]

669 See section 6.6.5.1 and section 6.6.5.4.
670 Dispatch regarding FinSA/FinIA, 8948.
671 See section 5.1.
672 See section 6.6.5.1.
673 See section 6.6.5.2.
674 Art. 58 and Art. 60 et seq. FinSA.
675 See also section 6.6.5.4.

6.6.4.3 Offer or public offer within the meaning of Article 3 letters g and h FinSA

If there is an invitation to purchase financial instruments and the information on this financial instrument is sufficiently detailed to enable the investors to accept the offer, this is considered to be an offer to purchase securities in accordance with Article 3 letter g FinSA. In other words, the offer must be (able to be) understood in good faith by investors.[676]

The term "public offer" is broadly defined in Article 3 letter h FinSA and also encompasses in particular offers of securities in the primary market, provided that they are not aimed at a restricted group of people.

If a company addresses a non-restricted group of persons in the context of an ICO with sufficiently detailed information on tokens that are classified as financial instruments and invites these persons to purchase the tokens in question, this is deemed a public offer in accordance with Article 3 letters g and h FinSA.

6.6.5 FinSA duties in case of an ICO

In view of the classification of ICOs under financial law set out in section 6.6.4, certain duties in FinSA may be relevant for a company making an ICO. The section below examines these duties in greater detail.

6.6.5.1 Prospectus requirement in accordance with Article 35 et seq. FinSA

The prospectus requirement applies to providers of securities within the meaning of Article 3 letter b FinSA and to persons that request the admission of securities for trading at a trading venue in accordance with Article 26 FMIA. The prospectus requirement is triggered either by a public offer, as defined in Article 3 letter h FinSA[677], or by a request for admission to trading at a trading venue.

For ICOs, the primary market is mainly relevant. If a company issues a notification to the public that contains sufficient information about the offer conditions and the token itself for a purchase or subscription of tokens as securities, this constitutes a public offer and hence is subject to the duty to the publication of a prospectus, unless the offer is exempt in accordance with Article 36 et seq. FinSA.[678]

6.6.5.2 Content of prospectus in accordance with Article 40 et seq. FinSA

In order to meet the protective aim underlying the prospectus requirement, the prospectus should contain full details of the issuer, the guarantor and the securities in a readily understandable form, and such details should be as objective and up to date as possible in order to enable investors to make an investment decision in full knowledge of the facts and the investment risks.

The prospectus should include information about the issuer – or on any guarantors in the case of issues of debt instruments – in accordance with Article 40 paragraph 1 letter a numbers 1-4 FinSA, especially regarding:

– the governing bodies, not in a strictly formal sense of the term, but rather all bodies with a management, corporate-law supervision and audit function;

– the most recent annual financial statement, comprising the balance sheet, income statement and notes[679];

---

676 Dispatch regarding FinSA/FinIA, 8948.
677 See section 6.6.4.3.
678 See section 6.6.5.3.
679 Art. 959–959c CO

- the current business situation, if it has not been sufficiently described already in the financial statement;
- the main prospects, including details of the state of research and development and the market prospects in the key business areas;
- material risks, including any dependency on patents and licences or impending changes in the regulatory environment;
- material disputes, including impending or ongoing civil, criminal, arbitration or administrative proceedings[680].

The prospectus must contain detailed information about the securities and the offer itself:[681] the rights, obligations and risks[682] for investors with respect to the securities and the type of investment and estimated net earnings with respect to the offer must be indicated. Concrete information requirements are set out in FinSO (as currently in consultation) in even greater detail. It is planned that FinSO will contain appendices with templates both for individual prospectus types and for the key information document. Such templates seem to be practical and usable in the implementation of an ICO as well.

Furthermore, the prospectus must contain a summary that contains key information in a concise form and generally understandable language.[683] Both the prospectus and the summary included in the prospectus may be written in one of the three official Swiss languages or in English. While the summary itself must be clear and understandable, the prospectus may be more detailed and more complex, as it is generally aimed at experienced players in the financial market.

6.6.5.3 Exemptions from the prospectus requirement in accordance with Article 36 et seq. FinSA

Article 36 FinSA contains a definitive list of the various forms of public offer for which the prospectus requirement is not justified for the purpose of client protection and for reasons of proportionality. For example, in the case of offers in accordance with Article 36 letter a, c and d FinSA, investors do not require any special protection in view of their financial means.[684] In the case of offers that are targeted at a limited investor group in accordance with letter b, there is generally a close relationship between the investors and providers, which should largely rule out misuse.[685] Parliament has set the investor group size here at 500 people. Offers with a total value of a maximum of CHF 8 million over a period of 12 months (letter e) are also exempt. In this case, the limit of CHF 8 million corresponds to the EU's prospectus requirements.[686]

Article 37 and Article 38 FinSA set out additional possible exemptions by type of security and exemptions for admission to trading.

---

680 Regarding the entire paragraph, see Dispatch regarding FinSA/FinIA, 8974, 8974.
681 Art. 40 para. 1 let. b and c FinSA.
682 These basically comprise all the particular technical risks relating to blockchain and DLT.
683 Art. 40 para. 3 FinSA.
684 Because they are considered to be professional clients (Art. 36 let. a FinSA); because the investors are acquiring securities worth at least CHF 100,000 (Art. 36 let. c FinSA) or because the offer stipulates a minimum amount of CHF 100,000 (Art. 36 let. d FinSA).
685 Dispatch regarding FinSA/FinIA, 8971.
686 Art. 3 para. 2 let. B Prospectus Directive (Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the prospectus to be published when securities are offered to the public or admitted to trading and amending Directive 2001/34/EC (Text with EEA relevance)).

6.6.5.4 Key information document (KID) for financial instruments in accordance with Article 58 et seq. FinSA

In general, the issuer of a complex financial instrument must always draw up a KID in advance for offers to private clients.

As a minimum, a provisional KID must be available before financial instruments are subscribed for which a KID needs to be drawn up in accordance with Article 58 paragraph 1 FinSA and which are offered in the primary market for subscription by investors.[687]

In accordance with Article 60 FinSA, the KID should contain all the key details that investors need to make an informed investment decision and to compare products from different issuers – in some case from different sectors. The documentation must be brief and easy to understand.[688] The KID must also be a stand-alone document and be significantly different from marketing material.[689]

First and foremost, the key information must contain the name of the financial instrument and the identity of the issuer[690], so that there is clarity at the point of sale as to whether the product provider is also the issuer of the financial instrument. Additionally, investors need sufficient details on the type, properties and risks of the product, as well as transparency about all direct and indirect costs related to investment in the product.[691] The KID must disclose any limitations and disadvantages relating to redemption of the product – such as long terms or a lack of liquidity.[692] It must also indicate whether authorisation is compulsory for the product or whether the law sets out an authorisation requirement for the issuer or the guarantor.[693] Hence, the issuer must, for example, decide whether the instrument has the legal form of a collective investment scheme or a structured product and indicate this decision in the KID (labelling requirement).[694]

In accordance with Article 59 FinSA, shares and comparable securities, especially debt instruments without the character of derivatives, are exempt from the requirement to draw up a KID. Shares and debt instruments without the character of derivatives have been a traditional form of investment for centuries, and it can be assumed that the basic characteristics of these investment forms are familiar to clients, including private clients. Consequently, if a company intends to issue tokens as part of an ICO that constitute shares or share-like securities, there is no need for an information document to be issued. The same applies if tokens constitute debt instruments without the characteristics of derivatives (for example a plain vanilla bond or similar).

6.6.5.5 Review of the prospectus and publication in accordance with Article 51 et seq. and Article 64 et seq. FinSA

Any person that offers securities in a public offer for purchase or subscription or that applies for securities to be admitted for trading must first publish a prospectus in accordance with Articles 40 et seq. FinSA, except where an exemption provision applies.[695] Prospectuses must be reviewed prior to publication in accordance with the provisions of Articles 51 et seq.[696] There is no requirement to have KIDs reviewed. Reviews must be carried out by a reviewing entity

687 Dispatch regarding FinSA/FinIA, 8986.
688 See Art. 61 para. 1 FinSA; Dispatch regarding FinSA/FinIA, 8988.
689 Art. 61 para. 2 FinSA.
690 Art. 60 para. 2 let. a FinSA.
691 Art. 60 para. 2 let. b–d FinSA.
692 Art. 60 para. 2 let. e FinSA.
693 Art. 60 para. 2 let. f FinSA.
694 Dispatch regarding FinSA/FinIA, 8988.
695 See section 6.6.5.3.
696 Dispatch regarding FinSA/FinIA, 8980-8981.

approved by FINMA.[697] After approval, prospectuses are valid for a year for public offers or admission to trading at a trading venue.

The duty to publish a prospectus is set out in Article 64 et seq. FinSA. In accordance with this article, the prospectus must be published at the latest at the start of the public offer or on the admission to trading of the securities in question. The prospectus must also be deposited at the office of the review body after approval.[698]

The duty to publish a KID is set out in Article 66 FinSA and applies in addition to the publication of a prospectus. In principle, Article 66 paragraph 1 FinSA requires that if a public offer is made of a financial instrument for which the production of a KID is required[699], the KID must be published.

If the exemption provisions in Article 36 et seq. FinSA do not apply to an ICO, the issuer must draw up a prospectus with content in accordance with Article 40 et seq. FinSA, have it reviewed as indicated above and publish it before the start of the offer. Moreover, unless the exemption provisions in Article 59 FinSA apply, the issuer must draw up a KID and publish it prior to the start of the offer if its offer is targeted at private clients. As indicated above, the KID does not have to be reviewed.

6.6.5.6 Other duties in accordance with FinSA

In addition to the above-mentioned duties of the issuer, it is conceivable that other players might be involved in an ICO. For example, a bank might in the future wish to buy issued tokens in the primary market or the secondary market for clients in the context of a portfolio management agreement or investment advice.

In the case of all these activities that constitute financial services within the meaning of FinSA[700], the classification of tokens as financial instruments is crucial.[701] If tokens are classified as financial instruments, the conduct rules in Chapter 2 of FinSA[702] apply. This chapter sets out the regulatory conduct rules for financial service providers, which financial service providers must observe in the provision of financial services on a professional basis. In general, they must always act in the interest of their clients. This is also a requirement in mandate law.[703] Financial service providers, such as banks, that recommend tokens issued in an ICO to their clients (in the secondary market), sell such tokens to their clients or buy such tokens in the name of their clients are naturally subject to the above duties.[704]

6.6.6 Conclusion

In the opinion of the Federal Council, there is no current need for any changes within the scope of FinSA. The novel and complex nature of the various financial instruments in the blockchain area justify the prospectus requirement in order to provide appropriate client protection and also to uphold the reputation of the Swiss financial centre. The prospectus requirement also applies to the analogue world, and there are currently no obvious reasons to set out different prospectus requirements for different business models. Looking at the function of a prospectus, which is to facilitate the investment decisions of potential investors and ensure

697 Art. 52 FinSA.
698 See Art. 64 para. 1 let. a and b FinSA.
699 See section 6.6.4.3, in general always on issuing and offering financial instruments to private clients.
700 See section 6.6.2.3.
701 See section 6.6.2.2.
702 Art. 7–20 FinSA
703 See Art. 394 et seq. CO; Dispatch regarding FinSA/FinIA, 8952.
704 See section 6.6.3.

that all interested parties have the same information, there is also no reason for any concrete changes.

Furthermore, it should be noted that the issue of bonds may be deemed a bank activity if the requirement to publish a prospectus or key information document is not met, as these debt certificates and the acceptance of these deposits could no longer be considered exempt from classification as a public deposit.[705] Issuers can resolve this issue by producing a key information document (KID), at least on a voluntary basis, in accordance with Article 58 et seq. FinSA for issues of bonds that would not be eligible for exemption in accordance with Article 36 et seq. FinSA and Article 59 FinSA[706], so that accepted monies cannot be classified as a public deposit within the meaning of BankO.[707]

6.7 Collective Investment Schemes Act (CISA)

6.7.1 Introduction

Blockchain technology also has potential in the area of collective investment law, but is still at an early stage. This is probably also related to the fact that the law on collective investment schemes uses clearly predefined structures that only allow for innovative models to a limited extent. It is currently difficult to determine what issues exist in practice and hence what action needs to be taken. The key questions today are discussed below.

6.7.2 Current legal situation

6.7.2.1 Basic regulatory content of CISA

General

Collective investment schemes within the meaning of the Collective Investment Schemes Act (CISA; SR 951.31) are assets collected from investors for the purpose of collective investment, and which are managed (by third parties) for the account of such investors. The investment requirements of the investors are met on an equal basis. The key characteristic of collective investment schemes is thus the presence of assets, the collective investment pool, third-party management and the equal satisfaction of investors' needs.[708]

Collective investment schemes may be open- or closed-ended.[709] In the case of open-ended collective investment schemes, investors are entitled to request the redemption of their units and payment in cash at any time. By contrast, investors in closed-ended collective investment schemes do not have any legal right to redemption of their units at the net asset value. Open-ended collective investment schemes include contractual funds[710] and investment companies with variable capital (SICAVs)[711]. Closed-ended collective investment schemes include limited partnerships for collective capital investment[712] and investment companies with fixed capital (SICAFs)[713]. While contractual funds – as the name itself indicates – are collective investment schemes in contractual form, SICAVs, limited partnerships for collective capital investment and SICAFS are collective investment schemes in corporate form.

---

705 See Art. 5 para. 3 BankO.
706 See also no. 6.3.2.2.
707 See section 6.6.5.3 and section 6.6.5.4.
708 Art. 7 para. 1 CISA; see also Rayroux/Du Pasquier 2016: Art. 7 CISA no. 3.
709 Art. 25 et seq. or Art. 98 et seq. CISA.
710 Art. 36 et seq. CISA.
711 Art. 25 et seq. CISA.
712 Art. 98 et seq. CISA.
713 Art. 110 et seq. CISA.

Authorisation and approval requirements

Any party responsible for the management of a collective investment scheme, the safekeeping of the assets held in it or the distribution of the collective investment scheme to non-qualified investors must obtain FINMA authorisation in accordance with Article 13 CISA. The following must apply for authorisation: fund management companies, SICAVs, limited partnerships for collective investment, SICAFs, custodian banks of Swiss collective investment schemes, managers of collective investment schemes, distributors and representatives of foreign collective investment schemes.

The distribution of foreign collective investment schemes in or from Switzerland to non-qualified investors must be approved in advance by FINMA in accordance with Article 120 paragraph 1 CISA. Foreign collective investment schemes that are only distributed to qualified investors do not require approval. However, they must designate a representative and a paying agent for units distributed in Switzerland.[714]

The question of eligibility for authorisation and approval must be considered separately from the provisions on authorisation and approval requirements. Products must be designed as specified by the law in order to be eligible for approval. The same applies to CISA authorisation holders. They must meet all legal conditions to be eligible for authorisation.[715]

With the entry into force of FinIA, distribution authorisation will be discontinued, and the provisions on managers of collective investment schemes and on fund management will be moved from CISA to FinIA.[716] CISA will thus become a law on products and be more streamlined.

6.7.2.2 Regulation of Swiss crypto funds

In the context of crypto-based assets, it is useful to consider whether Swiss collective investment schemes may invest in digital assets, such as cryptocurrencies.

In the area of open-ended collective investments (contractual funds and SICAVs), only one of the four fund types set out in CISA (securities funds, other funds for traditional investments, other funds for alternative investments, real estate funds) may invest in tokens: other funds for alternative investments. This fund type is an open-ended collective investment scheme that has a typical risk profile for alternative investments in terms of the selected investments, structure, investment techniques and investment restrictions.[717] In general, the same investments are permitted for other funds for alternative investments as for other funds for traditional investments[718], in particular investments in securities, precious metals, real estate, commodities, derivatives, units of other collective investment schemes and other assets and rights. FINMA may also permit other investments for other funds for alternative investments, such as raw materials and related instruments.[719] The list in the law is not definitive, which means that FINMA may permit investment in cryptocurrencies and other tokens.[720]

The provisions on other funds for alternative investments apply analogously to SICAFs. FINMA may permit additional investments.[721]

---

714 Art. 120 para. 4 CISA.
715 See Jutzi /Schären 2014: 29 et seq.
716 See for details Dispatch regarding FinSA/FinIA, 8928.
717 Art. 71 para. 1 CISA.
718 Art. 69 para. 1 CISA, Art. 99 para. 1 CISO.
719 Art. 99 para. 2 CISO.
720 Regarding the term "assets", see Jutzi/Schären 2014: 33; Rayroux/Du Pasquier 2016: Art. 7 CISA no. 11.
721 Art. 123 CISO:

Limited partnerships for collective investment make investments in risk capital.[722] Additionally, alternative investments in particular are permitted.[723]

Hence, CISA does not rule out the possibility that tokens may be admitted as an investment for certain fund types and are thus eligible for approval. It should, however, be noted, that the institutions responsible for managing a collective investment scheme and the prescribed custodian bank must meet certain conditions based on the particular features of the specific asset class of the fund assets that they manage or hold in custody. In particular, CISA sets out organisational conditions for appropriate risk management. Furthermore, fund assets constitute special assets that are managed in trust in favour of investors and held in custody by the custodian bank. This means that where a collective investment scheme invests in tokens, there must in particular also be appropriate safekeeping. Each individual case must be examined to determine whether these conditions are met.

6.7.2.3 Distribution of foreign crypto funds in Switzerland

Another issue is how foreign crypto funds that are distributed in Switzerland are regulated. As mentioned above, before foreign collective investment schemes can be distributed to non-qualified investors in or from Switzerland, this must be approved by FINMA.[724] Foreign collective investment schemes that are only distributed to qualified investors do not require approval. However, they must designate a representative and a paying agent for units distributed in Switzerland.[725]

To be eligible for approval, a foreign collective investment scheme must comply with the definition of "collective investment scheme" stipulated in Article 119 CISA. The conditions for approval are set out in Article 120 paragraph 2 CISA. Checks must be carried out to ensure that foreign prudential regulations and provisions on investor protection are equivalent to Swiss regulations.[726] It should be noted in particular that a representative and a paying agent must be appointed in the case of units distributed in Switzerland.[727] The representative within the meaning of Article 123 et seq. CISA requires authorisation. The paying agent must be a bank within the meaning of BankA.

This regulation also applies to foreign crypto funds. In accordance with this regulation, they can be approved or admitted for distribution in Switzerland, but the design of the fund plays a key role in individual cases. FINMA has not yet admitted any crypto funds for distribution in Switzerland. However, this is related to the fact that such funds are generally aimed exclusively at qualified investors, which means that they do not need any approval for distribution in Switzerland.

Distribution activity with respect to a collective investment scheme under foreign law in Switzerland requires authorisation as a distributor,[728] unless the distributor already has another type of authorisation or equivalent foreign authorisation.[729]

It is not known which foreign fund types distributors offer in Switzerland – namely in the area of distribution to qualified investors – as there is no prudential supervision of distributors or an authorisation requirement for foreign funds, provided that the investment funds in question are only offered to qualified investors in Switzerland.

---

722 Art. 103 CISA.
723 Art. 121 para. 1 let. b CISO.
724 Art. 120 para. 1 CISA.
725 Art. 120 para. 4 CISA.
726 See Jutzi/Schären 2014: 269.
727 Art. 120 para. 2 let. d CISA.
728 Art. 13 para. 2 let. g CISA.
729 Art. 19 para. 1bis CISA.

In 2018, FINMA issued distributor authorisation to an institution with its registered office in Switzerland to distribute a crypto fund domiciled offshore to qualified investors. In autumn 2018, FINMA granted the same institution authorisation as a manager of collective investment schemes, which means that it is now permitted to manage such crypto funds too.

6.7.2.4 Recording of fund units on a blockchain

Another possible need is to be able to record fund units on the blockchain. The aim of this would be to make unit settlement and register-keeping more efficient, as well as to improve tradability. The questions this raises are not specific to CISA and should be considered in the general regulatory context.[730] Most fund units of open-ended collective investment schemes are currently booked as intermediated securities.

Under the current collective investment schemes law, this kind of recording of units of collective investment schemes is not in itself forbidden. A token can theoretically also be a unit of a collective investment scheme. In other words, units of collective investment schemes can theoretically be recorded on a blockchain, in the same way as shares, for example. It must be noted, however, that open-ended collective investment schemes and SICAFs must have a custodian bank.[731] The custodian bank is responsible, among other things, for the task of issuing and redeeming units pursuant to the law.[732] Accordingly, it is not possible under current law to abstain from using a custodian bank by recording units of collective investment schemes on the blockchain. It is questionable whether the function of a custodian bank can be exercised via blockchain.

Finally, it must be pointed out that the issue of units of collective investment schemes in the form of shares on a blockchain must be examined for compliance with the pertinent provisions of the Swiss Code of Obligations.

6.7.2.5 Recording of the fund's assets on a blockchain

Finally, the question can be asked as to whether fund's assets can be recorded on the blockchain. However, this is not a CISA-specific question, either. It must be clarified for other institutions too whether their assets can be recorded on the blockchain. The question must therefore be considered in the general regulatory context.[733] Another problem is that it is not clear whether and how the functions of the authorisation holders, especially the fund management company and custodian bank, can be exercised if a fund's assets are recorded on the blockchain.[734]

6.7.2.6 Decentralised autonomous organisations (DAO) / funds on the blockchain

It is theoretically conceivable that in future not just units of collective investment schemes but the entire collective investment scheme, including the functions necessary for operations, management, custody and distribution in accordance with CISA, are recorded on the blockchain. The development of decentralised autonomous organisations (DAOs) is also heading in this direction. In very simple terms, DAOs are structures into which investors pay a cryptocurrency and which issue tokens in return that give investors participation rights. The community of token holders (investors) can then decide by e-voting (voting procedure is predefined and fixed in the software code) how the pooled assets are to be used (activities defined in advance and programmed in the software code). Once this decision has been taken, a smart contract implements it. Unlike conventional companies, DAOs do not have a

730 See the comments on banking law (section 6.2) and on the term "securities" (section 6.4.2).
731 The exemption option in Art. 44a CISA is hardly likely to apply.
732 See Art. 73 para. 1 CISA.
733 See the comments on banking law (section 6.2) and on the term "securities" (section 6.4.2).
734 See section 6.7.2.2.

management (a management committee) or a registered office.[735] DAOs can take very different forms. The best-known[736] example of a DAO is "The DAO".[737]

The question can be asked as to how DAOs are to be treated by law. As well as the issue of classification in accordance with private law, there is also the issue of whether DAOs are to be treated as collective investment schemes and whether they must meet the conditions set out in CISA. There is also the question of whether a DAO can fulfil the functions for operations, management and custody, as well as the related rights and duties in CISA.

In accordance with the above, the legal definition of a collective investment scheme comprises the following four criteria: assets, collective investments, equal satisfaction of investors' needs and third-party management. A structure organised contractually or as a corporation whose main explicit or implicit aim is collective investment automatically fits the definition of collective investment scheme and thus comes under the scope of CISA and is subject to the authorisation requirement, provided that no exemption applies.[738]

Three of the above-mentioned conditions (assets, collective investment and equal satisfaction of investors' needs) are likely to be regularly fulfilled by DAOs.[739] The question remains as to whether the condition of third-party management is met. In substantive terms, third-party management comprises active management, i.e. the taking of concrete investment decisions. Purely administrative functions or predefined instructions on portfolio management do not constitute third-party management. These conditions must be examined in each individual case.

If a DAO had third-party management, it would be subject to but not eligible for authorisation. To be eligible, it would have to have a permitted form in accordance with current law.

6.7.3 Conclusion

It can be concluded from the above that there is no need for action with respect to any blockchain- or DLT-specific barrier to market entry that might result from the requirement for distributor authorisation. As mentioned, this requirement was discontinued with the adoption of FinSA. Moreover, there is currently no need for action with respect to the distribution of foreign crypto funds to qualified investors in Switzerland.

It should be noted with respect to crypto funds that the Federal Council instructed the FDF in September 2018 to draw up a draft consultation paper to amend the CISA so as to permit a new fund category (limited qualified investment funds or L-QIF). This category will not be subject to FINMA authorisation and will be available to qualified investors. This means that innovative products can be brought to the market much more rapidly and cheaply in future, thus promoting the attractiveness of the Swiss fund market. As part of the work on the draft consultation paper, the potential investment spectrum of L-QIF is currently being clarified.

---

735 For details, see Gyr 2017: margin no. 8 et seq.; Hess/Spielmann 2017: 172.

736 Unknown persons exploited a weakness in the programming code of "The DAO" in order to misappropriate crytpocurrencies for improper purposes. At the same time, the US Securities and Exchanges Commission (SEC) established in an investigation that the tokens issued by "The DAO" constitute securities in accordance with US law and thus should only have been offered within the scope of US securities law in accordance with the relevant provisions. In the case of "The DAO", the SEC refrained from taking any further measures. For details, see the investigation report of the SEC of 25 July 2017, which is available at: https://www.sec.gov/litigation/investreport/34-81207.pdf (status as of: 5.11.2018).

737 For details, see Gyr 2017: Mmargin no. 11 ffet seq.

738 Rayroux/Du Pasquier 2016: Art. 7 CISA no. 15

739 For more on the classification of "The DAO" as a collective investment scheme, see Gyr 2017: margin no. 37 et seq.

Moreover, the use of blockchain technology in the area of collective investment law and the determination of the questions relating to the blockchain are, as mentioned above, still at a very early stage, which means that it is not possible to reach a definitive conclusion about the need for action at present. In particular, it is still unclear today how the institutions responsible for the operation of a collective investment scheme (especially the fund management company and the custodian bank) can fulfil their duties (such as controlling and due diligence duties) when using blockchain technology and whether the use of a custodian bank can be waived and, if so, under what conditions. It is essential to follow further developments and to quickly propose or implement any necessary regulatory measures. It should be noted that many of the questions that have arisen are not specific to CISA, but must be dealt with in studies across all relevant areas of law.[740]

This also applies to the legal classification of DAOs and any need to be able to record collective investment schemes in a completely new form on the blockchain. In this context, it should be noted that it is generally expected that there will be broadly autonomous software systems in the not too distant future that can take and implement business and other decisions independently. Accordingly, it will be necessary to clarify how to deal with such systems under private law and in particular whether they need to become legally independent. Additionally, their liability under civil and criminal law in particular will have to be determined.[741] Any amendment to CISA to take account of DAOs must be in line with studies across all fields of law and must not pre-empt them.

6.8 Insurance and DLT

Blockchain technology has also met with considerable interest from the insurance industry.[742] Many projects are still at an early stage, however. Accordingly, no definitive assessment under financial market law is possible. Additionally, various current projects do not at present have any direct relationship to the Federal Act on Insurance Policies and the Federal Act on the Oversight of Insurance Companies. Specific issues, above all, would need to be clarified in the area of data protection.

Questions under financial market law could arise if insurance products were comprehensively recorded with a DLT-based solution, such as whether insurance companies can accept cryptocurrencies as a means of payment or hold currencies in tied assets or whether an insurance pool or an insurance operation even exists in the case of pure smart contracts. A direct need for an amendment to financial market law with respect to DLT and insurance cannot currently be predicted, however. The Federal Council will thus follow developments closely and take any measures if necessary.

740 See section 6.7.2.4 and section 6.7.2.5.
741 See Häusermann 2017: 204.
742 See section 3.7.

7 Combating money laundering and terrorist financing

7.1 Introduction

This chapter deals with the risks of money laundering and terrorist financing presented by crypto-based assets and ICOs. It starts with an overview of the existing legal basis. The key risks for Switzerland in this area will then be examined based on the risk analysis[743] of crypto-assets and crowdfunding carried out by the interdepartmental coordinating group on combating money laundering and the financing of terrorism (CGMF). Subsequently, it will be shown whether and how the existing legal bases are applicable to activities involving crypto-based assets and ICOs. Finally, the chapter outlines the need for action based on the risk and on an analysis of the applicability of legislation.

7.2 Terms and legal basis

7.2.1 Swiss Criminal Code

In accordance with Article 305bis Swiss Criminal Code, any person who carries out an act that is aimed at frustrating the identification of the origin, the tracing or the forfeiture of assets which he knows or must assume originate from a felony or aggravated tax misdemeanour is deemed to be laundering money. In accordance with Article 260^{quinquies} Swiss Criminal Code, any person who collects or provides funds with a view to financing a violent crime that is intended to intimidate the public or to coerce a state or international organisation into carrying out or not carrying out an act is financing terrorism.

There is no definition of assets in the Swiss Criminal Code. Nonetheless, the Federal Council stipulates in its dispatch with reference to Article 305bis Swiss Criminal Code that the term "assets" is to be interpreted broadly.[744] The Federal Supreme Court also uses a broad interpretation.[745] The legal opinion that seems to be most widespread classifies virtual currencies (and thus also cryptocurrencies) as assets.[746] The Federal Council also concluded, in its report of 25 June 2014, that virtual currencies are to be considered as assets in view of their tradability.[747] In the opinion of the Federal Council, cryptocurrencies, such as Bitcoin, are to be deemed virtual currencies.[748] As the definition of virtual currencies in the Federal Council's report on virtual currencies is based on the characteristics of the Bitcoin, other cryptocurrencies with the above characteristics are also to be classified as virtual currencies.[749]

In connection with the term "originate" in the definition of money laundering in Article 305bis Swiss Criminal Code, the question arises as to how far away an asset can "originate" from a felony and still be contaminated. If the interpretation is too broad, a significant portion of the

---

743 See CGMF 2018a.

744 BBl **1989** II 1061, 1082. It is intended [...] to cover not just money in all forms and currencies, but also certificated securities, creditor rights, precious metals and stones, all other kinds of movable property, and even real estate and related rights.

745 See z. B. BGE **120** IV 365, Point 1d: "The assets that may be subject to forfeiture in accordance with Art. 58 Swiss Criminal Code are all economic benefits that can be calculated mathematically and that are obtained directly or indirectly by means of criminal acts".

746 See Scholl 2018: 360 ff; Müller/Reutlinger/Kaiser 2018: 86 f; Simmler/Selman/Burgermeister 2018: 963 et seq.

747 See Report on virtual currencies: 7–8. The term "virtual currency" is defined there as a digital representation of an asset that can be traded on the Internet and assumes certain functions of money in that it can be used as payment for real goods and services but it is not considered legal tender anywhere. Unlike coins or banknotes and sight deposits at the SNB, cryptocurrencies are not accepted as legal tender and are not denominated in Swiss francs (e.g. BTC, ETH).

748 Report on virtual currencies: 8-9.

749 See also Essebier/Bourgeois 2018: 573.

legal economy would be contaminated. If it is too narrow, there could be a conflict with access by the law enforcement authority.[750]

7.2.2 Anti-Money Laundering Act and Anti-Money Laundering Ordinance[751]

Financial intermediaries and dealers

The Anti-Money Laundering Act of 10 October 1997 (AMLA)[752] applies to both financial intermediaries and dealers that accept cash of more than CHF 100,000 as part of a commercial transaction. Financial intermediaries are considered in general to be persons that on a professional basis[753] accept or hold on deposit assets belonging to others or who assist in the investment or transfer of such assets[754], in addition to financial institutions subject to authorisation in accordance with special legislation.[755] This includes persons that provide services related to payments on a professional basis.[756] Professional money changing is also subject to AMLA.[757]

The applicability of AMLA to professional services relating to payments is particularly relevant to this topic and will therefore be examined in greater detail below. The Anti-Money Laundering Ordinance of the Federal Council of 11 November 2015[758] (AMLO) indicates how a "service relating to payments" is to be interpreted. In accordance with Article 4 paragraph 1 AMLO, a service constitutes a service relating to payments if the financial intermediary:

– transfers liquid financial assets to a third party on behalf of its contractual party and hence takes possession of such assets, has them credited to its own account or issues instructions for the transfer of the assets in the name and on behalf of the contractual party;

– issues or manages cashless means of payment, and its contractual party uses these to make payments to third parties;

– carries out money or asset transfer transactions.

The professional issue of a cashless means of payment is thus a financial intermediary activity. A definitive list of means of payment does not exist under Swiss law. Article 2 paragraph 3 letter b AMLA cites credit cards and travellers' cheques as examples of means of payment within the meaning of AMLA. The examples given in Article 2 paragraph 3 letter b AMLA are of means of payment that are or were previously widely used (travellers' cheques are no longer widely used in Switzerland). In its dispatch[759], the Federal Council indicates that in accordance with paragraph 3 letter b, other services, as well as the payment services of the PTT (now Swiss Post), come under the scope of the law if there is direct client contact. This applies in particular to credit cards, travellers' cheques and bank cheques. The non-definitive list of means of payment leaves open the option of new forms of means of payment. In accordance with Article 4 paragraph 2 AMLO, means of payment are instruments that allow third parties to transfer assets. The article mentions some examples, including virtual currencies. The issue

750 See Taube 2013: 88; Stratenwerth 2000: 339.
751 The provisions of the former Ordinance of the Federal Council on the professional exercise of financial intermediary activity of 18 November 2009 (SR **955.071**; applicable until 1 January 2016) were integrated into the Anti-Money Laundering Ordinance.
752 SR **955.0**
753 Art. 7 AMLO.
754 Art. 2 para. 3 AMLA.
755 Art. 2 para. 2 AMLA.
756 Art. 2 para. 3 let. b AMLA in conjunction with Art. 4 AMLO.
757 Art. 2 para. 3 let. c AMLA in conjunction with Art. 5 para. 1 let. a AMLO.
758 SR **955.01**
759 BBl **1996** III 1101, 1118.

of means of payment is only subject to AMLA if the issuing office is not identical with the users of the means of payment, that is, if there is (at least) a trilateral relationship.[760] FINMA applies the article to all means of payment whose value is fixed at the time of issue.[761] This is also the case for cryptocurrencies such as Bitcoin and Ether.

The money or asset transfer business is basically always professional and thus constitutes a financial intermediary activity within the meaning of AMLA.[762] Article 4 paragraph 2 AMLO defines the money or asset transfer business as including the transfer of assets by means of the acceptance of cash, precious metals, virtual currencies, cheques or other means of payment and:

a. payment of a corresponding amount in cash, precious metals or virtual currencies; or
b. cashless transfer via a payment or clearing system

Before taking up business, financial intermediaries subject to AMLA must become affiliated to a self-regulatory organisation (SRO) recognised by FINMA or apply for FINMA authorisation as a directly subordinated financial intermediary (DSFI).[763] They are subject to the duties of due diligence and duties in the event of a suspicion of money laundering.[764]

Due diligence duties[765]

Financial intermediaries must observe duties of due diligence to prevent money laundering and terrorist financing, as well as duties in the event of a suspicion of money laundering. Due diligence duties include clarifying the type and purpose of the business relationship, namely:

1. Verifying the identity of the contractual party by means of a document of evidentiary value (I.D. card for individuals, extract from the Register of Commerce or articles of association for legal entities).[766]
2. Determining the beneficial owner of the deposited assets.[767]
3. Verifying the identity or determining the beneficial owner again, for example due to doubts about the identity of the contractual party or the beneficial owner arising during the business relationship.[768]
4. Special duties of due diligence. In the case of business relationships with increased risk (for example politically exposed persons or clients headquartered in a high-risk country), additional clarifications must be carried out. These additional clarifications must include obtaining additional background information on the business relationship. The origin, purpose or background of the deposited or withdrawn assets, the source of the assets or the business activities of the client or the beneficial owner must be clarified, depending on the circumstances.[769]
5. Documentation and safekeeping obligation[770]
6. Organisational measures[771]

---

760 See FINMA Circ. 2011/1: Margin no. 64.
761 See FINMA Circ. 2011/1: Margin no. 64.
762 Art. 9 AMLO.
763 Art. 14 para. 1 AMLA.
764 The focus in the next section is on financial intermediaries, so there is no further discussion of dealers.
765 Art. 3 to 8 AMLA.
766 Art. 3 AMLA.
767 Art. 4 AMLA
768 Art. 5 AMLA.
769 Art. 6 AMLA.
770 Art. 7 AMLA.
771 Art. 8 AMLA.

Duties in the event of a suspicion of money laundering

The duties in the event of a suspicion of money laundering require financial intermediaries to report suspicions to the Money Laundering Reporting Office Switzerland without delay. Financial intermediaries must submit a report if they know or have reasonable grounds to suspect that the assets involved in the business relationship are related to money laundering, stem from a crime, are subject to the power of disposal of a criminal organisation or are used for terrorist financing.[772]

7.2.3 FINMA Anti-Money Laundering Ordinance

The Ordinance of FINMA of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism in the Financial Sector (AMLO-FINMA)[773] sets out how DSFIs[774] are to implement the duties involved in combating money laundering and terrorist financing. It stipulates what the general duties of due diligence are for such financial intermediaries, when such duties do not apply and when simplified duties of due diligence apply, as well as setting out provisions on special duties of due diligence.

FINMA can take into account the particular features of financial intermediary activity and can approve a relaxation or a tightening of the provisions, depending especially on the money laundering risk of an activity or the size of a company. It can also give consideration to the development of new technologies that offer equivalent security for the implementation of due diligence duties.[775]

Due diligence duties

Article 10 AMLO-FINMA stipulates the details necessary for payment orders. In accordance with Article 11 AMLO-FINMA, financial intermediaries with long-term business relationships with contractual parties in the area of cashless payment transactions that are exclusively intended for the cashless payment of goods and services are not subject to due diligence duties unless specific maximum amounts per transaction, month and year are exceeded. Article 12 AMLO-FINMA sets out the simplified due diligence duties for issuers of means of payment. Articles 13–21 AMLO-FINMA contain the special duties of due diligence. Article 13 and Article 14 AMLO-FINMA require financial intermediaries to develop criteria that point to business relationships or transactions with increased risk. Criteria that are particularly relevant in the crypto area include a lack of personal contact to the contractual party or to the beneficial owner, as well as the type of services and products requested. If financial intermediaries become aware of such circumstances, they must carry out further clarifications[776] and check the results of such clarifications to ensure their plausibility.[777] Business relationships and transactions must be monitored.[778] Certain financial intermediaries, including DSFIs[779], are subject to special provisions with respect to due diligence duties.[780]

772 Art. 9 to 11 AMLA.
773 SR **955.033.0**
774 See Art. 2 para. 2 let. a–d AMLA as well as Art. 2 para. 3 AMLA.
775 Art. 3 para. 2 AMLO-FINMA.
776 Art. 15 AMLO-FINMA.
777 Art. 16 AMLO-FINMA.
778 Art. 20 AMLO-FINMA.
779 Art. 44 bis Art. 76 AMLO-FINMA.
780 Art. 35 bis Art. 76 AMLO-FINMA.

7.3 Risks

As the relevant report shows[781], it is not easy to assess the risk of money laundering and terrorist financing using cryptobased assets[782] in Switzerland. The threat[783] associated with cryptobased assets is real and proven. It affects all countries, and not only Switzerland. Similarly, the vulnerabilities[784] with regard to the risks of cryptobased assets are considerable for Switzerland as well as for other countries. Nevertheless, a low number of cases of money laundering using cryptobased assets have been detected in Switzerland to date and no cases of terrorist financing using cryptobased assets have been recorded, although it is not known whether the small number is the result of a low actual risk overall or the difficulty of identifying transactions involving cryptobased assets with a criminal background.

7.3.1 Threats in relation to cryptobased assets

In many cases, the use of cryptobased assets simply adds to the complexity of crime patterns that exist independently of them. However, cryptobased assets and their underlying technology pose a new threat.

7.3.1.1 Threat inherent in the technology for cryptobased assets

The biggest threat in relation to cryptobased assets concerns primarily the anonymity in the sense of anti-money laundering law[785] which is associated with related transactions. In this respect, the risk is similar to that associated with cash.[786] However, it is further accentuated by the speed and mobility of the transactions made possible by the underlying technology. Cryptocurrencies allow huge sums to be transferred from one electronic account to another in a matter of seconds without anyone knowing who is initiating the transaction. In addition, private cryptographic keys that give access to wallets can be transmitted online to third parties on the other side of the world. In this way, anonymous users are able to access the amounts in question almost immediately, wherever they are. The risk of money laundering using cryptocurrencies is due to the combination of anonymity, speed and mobility.

7.3.1.2 Cryptobased assets and traditional financial crime

Cryptobased assets could become a major threat in terms of terrorist financing. Although no such cases have been identified in Switzerland to date and only a few examples have been identified at the international level[787], the threat posed by cryptocurrencies is illustrated by the many calls for cryptocurrency donations made by Islamic State (IS) supporters and the tutorials that some of them have posted online to explain to IS sympathisers worldwide how to conduct cryptocurrency transactions in favour of the organisation's wallets.[788]

The sale of illegal goods and services on the darknet also constitutes a significant money laundering threat associated with cryptocurrencies. The presumed connection between darknet trading venues and cryptocurrency price movements likewise attests to this.[789]

---

781 For more details, see CGMF 2018a.
782 The term "cryptobased assets" is synonymous with the term "crypto assets" used in the CGMF 2018a report.
783 Threats are defined as the probability of a person or a group of people committing acts of money laundering or terrorist financing.
784 Vulnerabilities are the set of (structural and institutional) factors that make the commission of a felony appealing to a person or group of people who wish to launder money or contribute to the financing of terrorist acts.
785 From an anti-money laundering law perspective, this refers in particular to constellations where the beneficial owner of the assets is not known.
786 See CGMF 2018b for further details.
787 European Parliament 2018: 29.
788 Wile 2014; Brantly 2014: 4.
789 See Bank for International Settlements, BIS Annual Economic Report 2018, dated 24 June 2018, 107, chart V.9, 107. Available at www.bis.org > Research & Publications > Annual Economic Report > Annual Economic Report 2018 (as at 18 October 2018).

7.3.2 Money laundering and terrorist financing risks in relation to ICOs

ICOs pose a similar threat in terms of money laundering and terrorist financing to cryptobased assets in general. Like these, they can be used to invest funds of criminal origin. To the extent that the cryptobased assets issued by ICOs are deemed equivalent to means of payment and are exchangeable into other cryptocurrencies, they could facilitate the laundering of cryptobased assets of criminal origin or increase the complexity of money laundering transactions involving cryptobased assets. Furthermore, even though no such cases have been identified in Switzerland to date, it cannot be ruled out that ICOs could be used as a cover for fundraising campaigns to finance terrorist organisations or activities. The reported or suspected cases of ICO abuse mostly concern investor fraud, though.

7.3.3 Switzerland's vulnerabilities with regard to money laundering and terrorist financing via cryptobased assets

In view of the real danger of money laundering and terrorist financing using cryptobased assets, the vulnerabilities of Switzerland are considerable, as are those of all countries.

The vulnerabilities relate primarily to the difficulty of identifying the beneficial owners of cryptobased assets in individual wallets. As many transactions take place via providers that are not considered financial intermediaries, especially non-custodian wallets and decentralised trading platforms, the identity of those who initiate them is not known. Regarding decentralised trading platforms, for example, certain categories of decentralised trading platforms are not subject to the AMLA in Switzerland.[790] Abroad, decentralised trading platforms are usually not subject to the anti-money laundering regulations in force there. Moreover, transactions and exchange transactions in cryptobased assets are often carried out through service providers registered in different jurisdictions, where the application of anti-money laundering regulations to such transactions can vary significantly. In principle, only exchange transactions between fiat currencies and cryptobased assets allow for secure identification of the beneficial owner.

The second key vulnerability of the financial system with regard to cryptobased assets both in Switzerland and abroad concerns the difficulty of identifying the criminal background of a transaction. Although chain analysis instruments can be used to trace the history of some transactions involving cryptobased assets – even if it is incomplete due to mixing – it is difficult to identify their possible criminal origin.

These two vulnerabilities, which are not specific to Switzerland, are important for financial intermediaries and criminal prosecution authorities, for whom the cross-border dimension of transactions in cryptobased assets is a particular obstacle.

7.3.4 Risk analysis conclusion

Even though the risks carried by cryptobased assets for money laundering and terrorist financing cannot be formally assessed due to the small number of reported cases, the CGMF report on the subject shows that the threat they pose is real and proven and that Switzerland's vulnerabilities in this regard are considerable. However, Switzerland is not alone. The threat and vulnerability are characterised by their cross-border dimension and affect all countries.

7.4 Applicability of the Anti-Money Laundering Act to activities in the crypto area

This chapter analyses which activities are subject to anti-money laundering legislation in Switzerland and determines which activities are not subject to AMLA. The AMLA is neutral with

---

790 This concerns particularly platforms where only supply and demand are brought together and where the platform operator has no power of disposal and is not itself a counterparty to the respective exchange transactions.

respect to technology and defines which activities can be defined as financial intermediary activity, irrespective of the means used. Consequently, activities that constitute financial intermediary activities in the analogue world basically also constitute financial intermediary activities in the virtual world. Given that the characteristics of cryptocurrencies[791], as described in section 7.2.1, are similar to those of money and that the risks entailed are also similar, it would seem appropriate to apply the same anti-money laundering provisions to cryptocurrencies as to conventional currencies.

7.4.1 Applicability of the Anti-Money Laundering Act to activities involving cryptocurrencies

Before the activities carried out by the individual players with respect to cryptocurrencies are examined, it must be noted that, as with other means of payment, the payment of goods and services in cryptocurrencies and the provision of services in return for payment in cryptocurrencies do not constitute financial intermediary activity and are therefore not subject to AMLA.[792]

7.4.1.1 Wallet providers

Custodian wallet providers

Custodian wallet providers hold clients' private keys in safekeeping and enable clients to send and receive cryptocurrencies. They have power of disposal over third-party assets, so that they can trigger transactions.[793]

If custodian wallet providers order the transfer of cryptocurrencies in the name and on behalf of contractual parties, they are providing a payments transaction service.[794] This means that they must be affiliated to an SRO or be directly subject to FINMA supervision. Like other financial intermediaries subject to AMLA, custodian wallet providers must fulfil the duty of due diligence in accordance with AMLA. Based on FINMA practice, the requirements may be loosened occasionally in accordance with Article 12 paragraph 2 letter d AMLO-FINMA.

Non-custodian wallet providers[795]

Unlike custodian wallet providers, the providers of non-custodian wallets do not keep or have access to clients' private keys. Non-custodian wallet providers can neither view nor access clients' wallets. Providers merely make software available and are not involved in the transfer of assets. Clients can transfer cryptocurrencies without the involvement of their non-custodian wallet providers. Such transfers are peer-to-peer transactions. Such activities cannot be readily described as financial intermediary activities in accordance with applicable law and hence be considered subject to AMLA, even under a broad interpretation of Article 2 paragraph 3 AMLA. As non-custodian wallet providers do not have any power of disposal (either in law or in practice) over the third-party assets, they do not meet the criteria to be classified as financial intermediaries.[796] Consequently, the Federal Council does not consider them to be subject to AMLA.

---

791 "[Cryptocurrencies] are units of value that can be used to pay for real goods and services, that are accepted by a community as a means of payment and that have a financial value independent of their intrinsic value", see Report on virtual currencies: 14.

792 Report on virtual currencies: 14.

793 See section 2.4.

794 See section 7.2.2

795 See section 2.4.

796 See FINMA Circ. 2011/1: Margin no. 7, margin no. 58, margin no. 119; Ruling of the Federal Supreme Court 2A.62/2007 of 30 November 2007 E.4.

7.4.1.2 Trading platforms

Central trading platforms

Central trading platforms[797] keep an order book and bring the supply and demand of their market participants together by means of matching. Trading platforms hold assets for their clients in their own wallets. They generally have access to clients' private keys and therefore also have power of disposal over third-party assets. As the trading platform accepts money or cryptocurrencies from clients and transfers them to other clients, thereby acting as an intermediary between clients in a trilateral relationship, it can be considered to be providing a service relating to payments.[798] It can therefore be classified as a financial intermediary and must fulfil the due diligence duties set out in AMLA. Based on FINMA practice, the duty of identification and the duty to identify the beneficial owner apply from CHF 0, as is the case with foreign transfers by money transmitters, as such transfers cannot be restricted geographically.[799] Trading platforms that only bring together buyers and sellers but do not carry out any activities that can be classified as financial intermediary activities are not subject to AMLA.[800]

Decentralised trading platforms

Decentralised trading platforms[801] do not have access to clients' private keys and so do not have direct power of disposal over third-party assets. Cryptocurrencies are held decentrally in clients' wallets. The trading platform combines supply and demand in the same way as central trading platforms. However, transactions are settled directly on the blockchain between clients with the help of smart contracts, which withhold the cryptocurrency amounts transferred for trading purposes until the transactions are signed by the users.[802] In some cases the platform must confirm or approve orders in order to ensure smooth trading and it can also block orders.[803] Based on the concept of financial intermediary activity and current FINMA practice, financial intermediaries must have power of disposal over third-party assets. The applicability of AMLA thus depends on whether platforms have the option of influencing clients' transactions.

In the case of decentralised trading platforms, trades – that is, the mutual transfer of traded tokens – are settled via smart contracts. Smart contracts are generally operated by the corresponding trading platform and contain corresponding technical controls and ways of exerting influence. Based on FINMA practice, decentralised trading platforms in such constellations are basically subject to AMLA, as they can dispose of third-party assets by confirming, approving or blocking orders.[804] If the trading platform facilitates the transfer of assets via a smart contract that it operates, which gives it access to orders via the smart contract, this can be seen as assistance in the transfer of assets and especially as a service relating to payments within a broad interpretation of power of disposal over third-party assets.[805] If, on the other hand, trading platforms bring buyers and sellers together and transactions are settled completely decentrally without trading platform access via a smart

797 See section 2.4.
798 Art. 2, para. 3 let. b AMLA in conjunction with Art. 4 AMLO, Report on virtual currencies: 16.
799 Based on Art. 52 and Art. 62 AMLO-FINMA, see also Report on virtual currencies: 17.
800 Report on virtual currencies: 15.
801 See section 2.4.
802 The transfer can also take place via off-chain payment systems. In such cases, the payment system or the operator have no power of disposal over users' assets. Users transfer cryptocurrencies to each other with the help of the payment system infrastructure.
803 A fully decentralised platform does not have this option, as the idea is that the trading takes place between clients directly, regardless of the platform.
804 Art. 2, para. 3 let. b AMLA in conjunction with Art. 4 AMLO.
805 This activity is thus subject to Art. 2 para. 3 AMLA.

contract, the activity in question is pure intermediation without any influence on payment flows. Such providers are not subject to the AMLA.[806]

7.4.1.3 Currency exchange offices

In currency trading, exchange offices sell and buy cryptocurrencies directly from their own holdings. There is a bilateral relationship between the exchange office and the client. The professional purchase and sale of cryptocurrencies in return for conventional currencies (e.g. CHF) or for other cryptocurrencies constitute exchange activities subject to AMLA[807]. FINMA currently uses a limit of CHF 5,000 for its identification requirement for currency exchange offices.[808] The contractual party must be identified from CHF 5,000 in the case of currency trading and from CHF 25,000 for all other cash transactions[809]. The exchange office must take appropriate measures to ensure that the wallet in question is the client's and not a third party's. Otherwise it would constitute a service relating to payments and the identification duty would apply from the amount of CHF 0.[810]

7.4.1.4 Crypto funds

Crypto funds are generally understood to be collective investment schemes that invest their assets primarily or exclusively in cryptocurrencies or other crypto-based currencies. They are treated the same as other collective investment schemes under anti-money laundering legislation, i.e. they are deemed to be financial intermediaries if they have authorisation as a fund management company, a SICAV, a limited partnership for collective investment or a SICAF.[811] More information about the applicability of CISA is available in the comments in section 6.7.

7.4.1.5 Mining

As confirmation of the authenticity of a transaction, miners receive either the originally issued token or a transaction fee (transfer of existing tokens). In the case of certain blockchains, this is a type of compensation for providing computing power to the network. There is no counterparty. If the tokens are to be used by the holder as a means of payment, they must be classified as "utility" and not as financial intermediary activity within the meaning of AMLA.[812]

7.4.2 Applicability of anti-money laundering legislation to activities involving ICOs

As AMLA is fundamentally neutral with respect to technology, it may also apply to activities involving ICOs, provided that such activities can be classified as financial intermediary activities. FINMA has published guidelines on ICOs[813], in which it defines different categories of tokens[814] and indicates whether they are subject to AMLA.

7.4.2.1 Payment tokens

The issue of payment tokens may come under Article 4 letter b AMLO, as they can be used to pay third parties for goods and services[815]. In accordance with FINMA guidelines, the issuing

806 Report on virtual currencies: 15.
807 See Report on virtual currencies: 14, FINMA 2018a: 7, FINMA-Circ. 2011/1: Margin no. 84. See also no. 7.2.2.
808 Art. 51 AMLO FINMA.
809 Art. 51 AMLO-FINMA; this limit is lowered to CHF 15,000 in the amended AMLO-FINMA that enters into force on 1 January 2020.
810 Art. 52 AMLO FINMA in conjunction with FINMA practice (see information on "*central trading platforms*").
811 Art. 2 para. 2 let. b and Art. 2 para. 2 let. b^{bis} AMLA.
812 See Grünewald 2015: 107-108; Müller/Reutlinger/Kaiser 2018: 89.
813 FINMA 2018a.
814 See section 6.2.
815 See also Kogens/Luchsinger 2018: 592. See also no.7.2.2.

of payment tokens constitutes the issuing of a means of payment subject to anti-money laundering provisions as long as the tokens can be transferred technically on a blockchain infrastructure.[816] A token issued in an ICO can be classified as a means of payment if it is to be used or intended by the issuer to be used as a means of payment for the purchase of goods or services. The financial intermediary must be affiliated to an SRO or be directly subject to FINMA supervision in accordance with AMLA. In accordance with FINMA practice, this requirement is deemed to be met if the payment means is accepted by a financial intermediary subject to AMLA in Switzerland and the said financial intermediary complies with the duty of due diligence.[817] Hence, the financial intermediary does not need to be affiliated to an SRO itself nor does the ICO organiser need to be directly subject to FINMA.[818]

7.4.2.2 Asset tokens

If tokens do not have the properties of payment tokens, but instead have the economic function of a share, bond or derivative financial instrument, the issue of such tokens is not subject to AMLA, as the direct placement of securities does not constitute a financial intermediary activity. Such asset tokens are classified as securities in accordance with FINMA practice, and the issuer of an asset token can therefore not be classified as a financial intermediary.[819] AMLA may nonetheless apply if activity can be classified as securities dealer activity in accordance with the SESTA definition in Article 2 paragraph 2 letter d AMLA. This may be the case in particular for asset token trading in the secondary market.

7.4.2.3 Utility tokens

The issue of tokens that solely provide access to a digital function or service and cannot be used as a means of payment is not subject to AMLA. The same is true for the issue of tokens that are primarily intended to provide access to a non-financial application of blockchain – "accessoriness"[820] (e.g. monitoring the authenticity of drugs on blockchain). In the case of hybrid tokens[821], AMLA must be observed if the activity in question is subject to AMLA.

7.5 Conclusion

According to the risk analysis carried out by CGMF, there is a risk that crypto-based assets could be misused for money laundering and terrorist financing, based on the exposure and vulnerability identified in Switzerland. Such exposure and vulnerability can be found in all other countries of the world too. However, the risk analysis also shows that the actual risk in Switzerland cannot be determined precisely in view of the low number of cases.

AMLA is sufficiently neutral with respect to technology at present to be able to apply to activities related to cryptocurrencies and ICOs to a large extent. The general principles of AMLA also apply for crypto-based assets. The activities of most players in the crypto area today can be classified as financial intermediary activities and are thus subject to the AMLA. This means that the scope of AMLA is already relatively comprehensive by international comparison. The Federal Council therefore believes that it is therefore not necessary to fundamentally revise AMLA specifically with respect to crypto-based assets. The applicability of AMLA to individual activities, such as the issue of cryptocurrencies as a means of payment could, however, be specified more clearly by means of an explicit mention in AMLO.

Nonetheless, AMLA cannot readily be applied to certain activities that do not fit the definition of financial intermediary activity. The Federal Council believes that an extension of the

816 A.A. Blockchain Taskforce 2018b: 20. In the opinion of the Blockchain Taskforce, the issuer must be involved in the settlement of the payment or in transactions with third parties relating to payment tokens.
817 In accordance with Art. 12 para. 1 AMLO-FINMA.
818 FINMA 2018a: 6–7.
819 FINMA 2018a: 6–7.
820 See Art. 2 para. 2 let. a no. 3 AMLO; FINMA Circ. 2011/1: margin no. 13 ffet seq.
821 See section 6.2.4.

activities subject to AMLA should essentially only be considered if such activities present a risk with respect to money laundering and/or terrorist financing.

The following specific activities in the crypto area are currently not subject to AMLA:

a) providers of non-custodian wallets;

b) certain decentralised trading platforms; and

c) the issue of pure asset and utility tokens.

Non-custodian wallet providers

Many transactions in cryptocurrencies take place via non-custodian wallets, which are not subject to anti-money laundering provisions either inside Switzerland or, as far as is known, outside Switzerland. The Federal Council is aware of the corresponding risk, but believes that it would not be expedient to make providers of non-custodian wallets subject to AMLA at the moment. As transactions are made on a peer-to-peer basis and providers of non-custodian wallets ultimately only provide software and do not have power of disposal of third-party assets, they cannot be deemed to be acting as financial intermediaries. Consequently, such providers are at present not subject to anti-money laundering provisions internationally either. FATF has clarified the application of its recommendations to cryptocurrencies and decided that the FATF standards should not be applicable to non-custodian wallets providers. Switzerland will keep a close eye on these risks and FATF developments.

Decentralised trading platforms

CMGT's risk analysis also shows that numerous transactions in cryptocurrencies take place via decentralised trading platforms.

The Federal Council is aware of this risk too. At present, AMLA applies not just to central trading platforms, but in part also to decentralised trading platforms, provided that they can access orders via a smart contract in which they are required to confirm or authorise orders and can also block orders. On the other hand, AMLA does not apply to fully decentralised platforms that do not have the power to dispose of assets and merely connect supply with demand. In this case, the power of disposal criterion is not met and so this activity cannot be considered as a financial intermediary activity. This corresponds to FINMA's current practice. The FATF has stipulated that its standards[822] apply to activities involving cryptocurrencies, but it has not yet explicitly commented on the applicability of its standards to decentralised trading platforms. As far as is known, decentralised trading platforms outside Switzerland are not generally subject to anti-money laundering provisions at the moment.

Against this backdrop, it seems necessary to set out more explicitly in law the current applicability of AMLA to decentralised trading platforms in order to provide greater clarity for market participants. Moreover, the Federal Council believes that further analysis is necessary to determine whether other trading platforms that do not have any power of disposal of third-party assets should be subject to AMLA, given the need for internationally coordinated measures in light of the FATF's current international work. The Federal Council will continue to observe the risks arising from the various technical forms of trading platforms and promote uniform standards in the relevant international committees. It must also be considered whether it is technically possible to make such trading platforms subject to AMLA. Additional

822 See the FATF recommendations of February 2012 (status as of: October 2018), available at: www.fatf-gafi.org > All Publications > FATF Recommendations > FATF Standards (status as of: 14.11.2018), specifically Recommendation 15 as well as the explanations in the FATF glossary of "Virtual Asset" and "Virtual Asset Service Provider".

amendments to anti-money laundering law may be necessary at a later date, in view of the FATF's clarification work.

Issue of pure asset and utility tokens

No need for action has been identified with respect to the issue of asset and utility tokens. Such activities can currently not be interpreted as financial intermediary activity. Additionally, no increased risk of money laundering has been identified in these activities.[823]

Conclusion

Given the above, the Federal Council intends to take the following steps:

- It will set out in further detail and explicitly adopt into law the current FINMA practice whereby decentralised trading platforms with the power to dispose of third-party assets are subject to AMLA;
- It will set out in further detail and explicitly adopt into law the applicability of Article 2 paragraph 3 letter b AMLA to the issue of crypto-based means of payment;
- Switzerland will in future continue its efforts in international committees to actively promote an internationally coordinated and effective defence mechanism to combat the risks of money laundering and terrorist financing by means of international standards.

823 For further details, see CGMF 2018a.

8 Summary of the comments received in the informal industry consultation

The working group cultivated an intensive dialogue with the private sector as part of its analyses. In particular, it carried out an informal consultation of the financial and fintech industry in September 2018 on the basis of a short paper;[824] this consultation was met with great interest. In more than 50 comments, the respondents welcomed the opportunity to participate, praised the commitment of the authorities, and to a large extent supported the general thrust of the proposals made. In accordance with the diversity of the participants in the consultation, the range of opinions expressed was broad in regard to many points. However, there was agreement on the importance of discussing the legal framework, the need for technology-neutral regulation, and a continuation of the open dialogue between authorities and the industry.

Most comments consider the future potential of DLT/blockchain technology to be great for the financial industry, although the technological and regulatory challenges and certain risks are recognised throughout. There are different opinions regarding the time horizon of the unfolding of this potential, with estimates between 2 and 10 years.

On the question of how it could be made easier for companies with fintech business models to establish business relationships with Swiss banks, the participants agreed that there was no need for regulatory adjustment. Some opinions welcomed in particular the recently published SBA guidelines.

In the area of civil law, most participants in the consultation responded positively to the proposed amendments to securities laws.[825] While some participants expressly welcomed the proposed restriction to freely transferable, securitisable rights, others expressed the wish that all rights including ownership of chattels should be representable. Some respondents also commented that legal amendments were not necessary to represent and transfer negotiable securities on a blockchain.

Most respondents consider an expressly regulated right to segregate crypto assets and other digital data in insolvency to be necessary or desirable as clarification to increase legal certainty. In the report, the Federal Council proposes the creation of such provisions.[826]

In financial market law, the recently introduced or imminent fintech measures in banking law were welcomed. Assessment of the *sandbox* concept diverged among the participants. While a majority is of the opinion that the concept is key to fintech and should be further developed (necessity of additional sandboxes in other areas in addition to banking law, increase in threshold values), some respondents were more critical and considered an assessment of the sandbox under banking law, which was introduced only in 2017, to be premature. In view of the open, not uncontroversial issues, no concrete proposal for a new sandbox was included in the report. Various sandbox approaches were specifically examined and rejected in the area of financial market infrastructures.[827] The FDF intends, however, to further analyse the question of potential further development or expansion of the existing sandbox under banking law – also on the basis of feedback from the industry consultation as well as international

824 See consultation document available at: https://www.admin.ch/gov/en/start/dokumentation/medienmitteilungen.msg-id-72001.html (as at 5 November 2018).
825 See section 5.1.
826 See section 5.2.
827 See section 6.4.7.

developments. This analysis will be done from a general perspective, not specifically or exclusively in regard to blockchain/DLT applications.

The proposal to create a new licence category for financial market infrastructures in the blockchain/DLT domain[828] is also intended to address industry concerns, in particular the need clearly expressed in the consultation that trading platforms for crypto assets should also be directly accessible to private customers. With regard to the classification of tokens as securities or derivatives, FINMA's ICO guidance was welcomed, but a majority of participants would like additional clarification. The Federal Council intends to create additional legal certainty on the question of whether derivative trading obligations also apply to derivatives in the form of tokens.[829] With regard to the FinSA and FinIA, the participants in the consultation do not recognise any specific need for adjustment in regard to blockchain applications. This assessment corresponds to that of the Federal Council.[830] According to the feedback from the consultation, there is great interest in being able to pursue blockchain-based business models in the area of collective investment law. The use of blockchain technology for this purpose is still at a very early stage, however, so that the Federal Council will monitor further developments in close contact with the industry and rapidly propose or implement any necessary regulatory measures.[831]

With regard to anti-money laundering law, the consultation discussed in particular the question of subordination under that law. The majority of participants rejected subordination under the AMLA of decentralised trading platforms without power of disposal over third-party assets as well as non-custodian wallet providers, although there were also some opposing views. The Federal Council is of the opinion that such questions of subordination under the AMLA do arise due to the potential risks, for example in the area of decentralised trading platforms. At the same time, the scope of application of the AMLA is already comparatively comprehensive in an international comparison, and the potential risks of individual activities not yet falling within the scope of the AMLA are issues of distinctive international nature that can and should be tackled effectively only at the international level.[832]

The Federal Council welcomes the intensive participation of interested parties in this consultation. The dialogue with the industry must continue to be cultivated actively and on a regular basis. The comments – some of which were extensive – were taken into account when finalising this report and assessing the need for action. In addition, they are intended to be taken into account also in the upcoming legal follow-up work suggested in the report, where they will provide useful appraisals for that purpose. The Federal Council is aware that the interests of the various stakeholders in the DLT/blockchain realm and the financial market are diverse and not always pulling in the same direction. The aim of all regulation must be to create the best possible framework conditions in Switzerland for providers and users of new – as well as existing – technologies. The integrity and good reputation of the Swiss financial centre and business location must continue to be ensured.

828 See section 6.4.7.
829 See section 6.4.9.
830 See section 6.5.3 and section 6.6.6.
831 See section 6.7.3.
832 See section 7.5.

9 Reference lists

9.1 Bibliography

AMSTUTZ, MARC / MORIN, ARIANE (2015): Einleitung vor Art. 184 ff. OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Wiegand, Wolfgang (eds.): Basler Kommentar Obligationenrecht I. 6th edition. Basel: Helbing & Lichtenhahn.

BACON, LEE / BAZINAS, GEORGE (2017): "Smart Contracts": The Next Big Battleground? In: Jusletter IT of 18 May 2017.

BAIRD, LEEMON (2016): The Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance. Can be accessed at: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf (as at 19.10.2018).

BARTHOLD, BEAT M. / SCHILTER, IRÈNE (2017): Art. 135 FinfraG. In: Sethe, Rolf / Favre, Olivier / Hess, Martin / Kramer, Stefan / Schott, Ansgar (eds.): Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG. Zurich: Schulthess.

BÄRTSCHI, HARALD (2013): Art. 6 BEG. In: Zobl, Dieter / Hess, Martin / Schott, Ansgar (eds.): Kommentar zum Bucheffektengesetz (BEG). Zurich: Schulthess.

BÄRTSCHI, HARALD / MEISSER, CHRISTIAN (2015): Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht. In: Weber, Rolf H. / Thouvenin, Florent (eds.): Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme. Zurich: Schulthess, 115–160.

BAUER, CHRISTOPH (2010): Parteiwechsel im Vertrag: Vertragsübertragung und Vertragsübergang, Zurich/St. Gallen: Dike.

BECK, BENJAMIN (2015): Bitcoins als Geld im Rechtssinne. In: NJW 2015/9, 580–586.

BECK, SUSANNE (2017): Der rechtliche Status autonomer Maschinen. In: AJP 2017/2, 183–191.

BENHAMOU, YANIV / TRAN, LAURENT (2016): Circulation des biens numériques: de la commercialisation à la portabilité. In: sic! 2016/11, 571–591.

BERTSCHINGER, URS (2015): Das Wertrechtebuch gemäss Art. 973c Obligationenrecht. In: Waldburger, Robert / Sester, Peter / Peter, Christoph / Baer, Charlotte M. (eds.): Law & Economics, Festschrift für Peter Nobel zum 70. Geburtstag. Bern: Stämpfli, 307-320.

BÖCKLI, PETER (2009): Schweizer Aktienrecht. 4th edition. Zurich: Schulthess.

BOHNET, FRANÇOIS / HÄNNI, LINO (2017): Art. 973c OR. In: Tercier, Pierre / Amstutz, Marc / Trigo Trindade, Rita (eds.): Commentaire romand Code des Obligations II. 2nd edition. Basel: Helbing Lichtenhahn.

BONOMI, ANDREA (2011): Art. 113 ff. LDIP. In: Bucher, Andreas (ed.): Commentaire romand Loi sur le droit international privé (LDIP) / Convention de Lugano (CL). Basel, Helbing Lichtenhahn.

BÖSCH, RENÉ (2013): Art. 973c OR. In: Zobl, Dieter / Hess, Martin / Schott, Ansgar (eds.): Kommentar zum Bucheffektengesetz (BEG). Zurich: Schulthess.

BRANTLY, AARON (2014): "Financing Terror Bit by Bit". In: CTC Sentinel 2014/10, 1-5. Can be accessed at: https://ctc.usma.edu/app/uploads/2014/10/CTCSentinel-Vol7Iss101.pdf (as at 19.10.2018).

BRÜNNLER, KAI (2018): Blockchain – kurz & gut. Heidelberg: dpunkt.

BUCHER, EUGEN (1988): Schweizerisches Obligationenrecht Allgemeiner Teil ohne Deliktsrecht. 2nd edition. Zurich: Schulthess.

CHRISTEN, BERNHARD / HAUCK, BERND (2012): Art. 1153–1155 OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar. Basel: Helbing Lichtenhahn.

COSTANTINI, RENATO (2012): Art. 108a. In: Honsell, Heinrich / Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar Wertpapierrecht. Basel: Helbing Lichtenhahn.

DAENIKER, DANIEL / WALLER, STEFAN (2011): Art. 2 BEHG. In: Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar Börsengesetz / Finanzmarktaufsichtsgesetz. 2nd edition. Basel: Helbing Lichtenhahn.

DASSER, FELIX (2016): Art. 145 IPRG. In: Honsell, Heinrich / Vogt, Nedim Peter / Schnyder, Anton K. / Berti, Stephen V. (eds.): Basler Kommentar Internationales Privatrecht. 3rd edition. Basel: Helbing Lichtenhahn.

DE CAPITANI, WERNER (2002): Allgemeine Bestimmungen, GwG. In: Schmid, Niklaus / Bernasconi, Paolo / de Capitani Werner (eds.): Kommentar Einziehung, Organisiertes Verbrechen, Geldwäscherei, Band II. Zurich: Schulthess.

DRESCHER, DANIEL (2017): Blockchain Grundlagen. Frechen: mitp.

EBERHARD, STEFAN / VON PLANTA, ANDREAS (2013): Art. 151 IPRG. In: Honsell, Heinrich / Vogt, Nedim Peter / Schnyder, Anton K. / Berti, Stephen V. (eds.): Basler Kommentar Internationales Privatrecht. 3rd edition. Basel: Helbing Lichtenhahn.

ECKERT, MARTIN (2016): Digitale Daten als Wirtschaftsgut: digitale Daten als Sache. In: SJZ 112 (2016) Nr. 10, 245–249

EGGEN, MIRJAM (2018): Was ist ein Token? In: AJP 2018/5, 558–567.

EGGEN, MIRJAM (2017a): Chain of Contracts – Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers. In: AJP 2017/1, 3–15.

EGGEN, MIRJAM (2017b): Verträge über digitale Währungen: Eine privatrechtliche Qualifikation von Rechtsgeschäften in oder mit digitalen Währungen. In: Jusletter of 4 December 2017.

EGGEN, MIRJAM (2009): Sicherheiten an Wertrechten – eine Untersuchung der Rechtslage ab Inkrafttreten des Bucheffektengesetzes. In: SZW 2009/4, 116–127.

ERBGUTH, JÖRN (2018): Datenschutz auf öffentlichen Blockchains. In: Jusletter IT of 22 February 2018.

ERNST, WOLFGANG (2016): Art. 925 ZGB. In: Honsell, Heinrich / Vogt, Nedim Peter / Geiser, Thomas (eds.): Basler Kommentar Zivilgesetzbuch II. 5th edition. Basel: Helbing Lichtenhahn.

ESSEBIER, JANA / BOURGEOIS, JANIQUE (2018): Die Regulierung von ICOs. In: AJP 2018/5, 568–579.

ESSEBIER, JANA / WYSS, DOMINIC A. (2017): Von der Blockchain zu Smart Contracts. In: Jusletter of 24 April 2017.

FAVRE, OLIVIER / KRAMER, STEFAN (2017): Art. 2 FinfraG. In: Sethe, Rolf / Favre, Olivier / Hess, Martin / Kramer, Stefan / Schott, Ansgar (eds.): Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG. Zurich: Schulthess.

FORSTMOSER, PETER (2005): Abschied vom Numerus clausus im Gesellschaftsrecht? In: Waldburger, Robert / Nobel, Peter (eds.): Wirtschaftsrecht zu Beginn des 21. Jahrhunderts, Festschrift für Peter Nobel zum 60. Geburtstag. Bern: Stämpfli, 77–98.

FRÖHLICH-BLEULER, GIANNI (2017): Eigentum an Daten? In: Jusletter of 6 March 2017.

FURRER, ANDREAS (2018): Die Einbettung von Smart Contracts in das schweizerische Privatrecht. In: Anwaltsrevue 2018/3, 103–115.

FURTER, ROBERT (2014): Art. 973c OR. In: Honsell, Heinrich (ed.): Kurzkommentar Obligationenrecht. Basel: Helbing Lichtenhahn.

FURTER, ROBERT (2012): Vor Art. 965–1155 OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar Wertpapierrecht. Basel: Helbing Lichtenhahn.

GAUCH, PETER / SCHLUEP, WALTER / EMMENEGGER, SUSAN (2014): Schweizerisches Obligationenrecht Allgemeiner Teil – Band II. 10th edition. Zurich: Schulthess.

GERVAIS, ARTHUR (2018): Vorteile und Probleme von Blockchains. In: digma 2018/2, 128–131.

GIRSBERGER, DANIEL / GASSMANN, RICHARD (2018): Art. 145 IPRG. In: Müller-Chen, Markus / Widmer Lüchinger, Corinne (eds.): Zürcher Kommentar IPRG. 3rd edition. Zurich: Schulthess.

GIRSBERGER, DANIEL / HERMANN, JOHANNES LUKAS (2015): Art. 164 ff. OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Wiegand, Wolfgang (eds.): Basler Kommentar Obligationenrecht I. 6th edition. Basel: Helbing Lichtenhahn.

GLARNER, ANDREAS / MEYER, STEPHAN D. (2017): Smart Contracts in Escrow-Verhältnissen. In: Jusletter of 4 December 2017.

GLESS, SABINE / KUGLER, PETER / STAGNO, DARIO (2015): Was ist Geld? Und warum schützt man es? In: recht 2015, 82–97.

GOBAT, SÉBASTIEN (2016): Les monnaies virtuelles à l'épreuve de la LP: Questions choisies à l'exemple du bitcoin. In: AJP 2016/8, 1095–1105.

GRAHAM-SIEGENTHALER, BARBARA / FURRER, ANDREAS (2017): The Position of Blockchain Technology and Bitcoin in Swiss Law. In: Jusletter of 8 May 2017.

GRÜNEWALD, SERAINA (2015): Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen. In: Weber, Rolf H. / Thouvenin, Florent (eds): Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme. Zurich: Schulthess, 107–108.

GYR, ELEONOR (2017): Dezentrale Autonome Organisation DAO. In: Jusletter of 4 Dezember 2017.

HAUSER-SPÜHLER, GABRIELA (2017): Innovation vs. Regulation – Compliance im Digital-Finance-Bereich. Zurich: Schulthess.

HAUSER-SPÜHLER, GABRIELA / MEISSER, LUZIUS (2018): Eigenschaften der Kryptowährung Bitcoin. In: digma 2018/1, 6–12.

HÄUSERMANN, DANIEL M. (2017): Autonome Systeme im Rechtskleid der Kapitalgesellschaft. In: AJP 2017/2, 204–212.

HESS, MARTIN / KALBERMATTER, ANDRÉ / WEISS VOIGT, ALEXANDRA, Art. 81 FinfraG. In: Sethe, Rolf / Favre, Olivier / Hess, Martin / Kramer, Stefan / Schott, Ansgar (eds.): Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG. Zurich: Schulthess.

HESS, MARTIN / LIENHARD, STEPHANIE (2018): Unautorisierte Zahlungen mit virtuellen Währungen? In: Emmenegger, Susan (eds.): Zahlungsverkehr – Beiträge zur Schweizerischen Bankrechtstagung 2018. Basel: Helbing Lichtenhahn, 156–176.

HESS, MARTIN / LIENHARD, STEPHANIE (2017): Übertragung von Vermögenswerten auf der Blockchain: Darstellung der technischen Grundlagen und der Übertragungsformen de lege lata et ferenda. In: Jusletter of 4 December 2017.

HESS, MARTIN / SPIELMANN, PATRICK (2017): Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht. In: Reutter, Thomas U. / Werlen, Thomas (eds.): Kapitalmarkt – Recht und Transaktionen XII. Zurich: Schulthess, 145–202.

HOFMANN, DIETER / KUNZ, OLIVER (2016): Art. 5 LugÜ. In: Oetiker, Christian / Weibel, Thomas (eds.): Basler Kommentar Lugano Übereinkommen. 2nd edition. Basel, Helbing Lichtenhahn.

HRUBESCH-MILLAUER, STEPHANIE / GRAHAM-SIEGENTHALER, BARBARA / ROBERTO, VITO (2017): Sachenrecht. 5. Aufl. Bern: Stämpfli.

HÜRLIMANN, DANIEL / ZECH, HERBERT (2016): Rechte an Daten. In: sui-generis 2016, 89–95.

HÜRLIMANN-KAUP, BETTINA (2018): Zahlung mit Bitcoins: Zahlung mit Sachen? In: Emmenegger, Susan (eds.): Zahlungsverkehr – Beiträge zur Schweizerischen Bankrechtstagung 2018. Basel: Helbing Lichtenhahn, 139–154.

ISLER, MICHAEL (2017): Datenschutz auf der Blockchain. In: Jusletter of 4 December 2017.

JACCARD, GABRIEL (2017): Smart Contracts and the Role of Law. In: Jusletter IT of 23 November 2017.

JUTZI, THOMAS / SCHÄREN, SIMON (2017): Art. 120 FinfraG. In: Sethe, Rolf / Favre, Olivier / Hess, Martin / Kramer, Stefan / Schott, Ansgar (eds.): Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG. Zurich: Schulthess.

JUTZI, THOMAS / SCHÄREN, SIMON (2014): Grundriss des schweizerischen Kollektivanlagenrechts. Bern: Stämpfli.

KAULARTZ, MARKUS / HECKMANN, JÖRG (2016): Smart contracts – Anwendungen der Blockchain-Technologie. In: CR 2016/9, 618–624.

KOGENS, RONALD / LUCHSINGER GÄHWILER, CATRINA (2018): Ein 360-Grad-Blick auf Token. In: Expert Focus 2018/8, 589–596.

KUHN, HANS (2016): Art. 965 ff. OR. In: Amstutz, Marc / Breitschmid, Peter / Furrer, Andreas / Girsberger, Daniel / Huguenin, Claire / Jungo, Alexandra / Müller-Chen, Markus / Roberto, Vito / Schnyder, Anton K. Z/ Trüeb, Hans Rudolf (eds.): Handkommentar zum Schweizer Privatrecht. 3rd edition. Zurich, Schulthess.

KUNZ, PETER (2014): Crowdfunding. In: Jusletter of 25 August 2014.

LANZ, MARTIN / FAVRE, OLIVIER (2009): Inhaberaktien in der Form von Wertrechten – Neue Möglichkeiten unter Art. 973c OR. In: GesKR 2009/4, 548–553.

LEIMGRUBER, DOMINIK / FLÜCKIGER, BJÖRN-GUNNAR (2017): Schweizer Fintech-Regulierung – Ein Überblick. In: Jusletter of 6 November 2017.

LEU, URS (2015): Art. 84 OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Wiegand, Wolfgang (eds.): Basler Kommentar Obligationenrecht I. 6th edition. Basel: Helbing Lichtenhahn.

LOERTSCHER, DENIS (2012): Art. 84. In: Thénévoz, Luc / Werro, Franz (eds.): Commentaire romand Code des Obligations I. 2nd edition. Basel: Helbing Lichtenhahn.

MARKUS, ALEXANDER R. (2014): Internationales Zivilprozessrecht. Bern: Stämpfli.

MAUCHLE, YVES (2017): Die regulatorische Antwort auf FinTech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen. In: SZW 2017/6, 810–830.

MAURENBRECHER, BENEDIKT / MEIER, URS (2017): Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen. In: Jusletter of 4 December 2017.

MEIER-HAYOZ, ARTHUR / FORSTMOSER, PETER / SETHE, ROLF (2018): Schweizerisches Gesellschaftsrecht. 12th edition. Bern: Stämpfli.

MEIER-HAYOZ, ARTHUR / VON DER CRONE, HANS CASPAR (2018): Wertpapierrecht. 3rd edition. Bern: Stämpfli.

MEINEL, CHRISTOPH / GAYVORONSKAYA, TATIANA / SCHNJAKIN, MAXIM (2018), Blockchain: Hype oder Innovation, Technische Berichte Nr. 113 des Hasso-Plattner-Instituts für Digital Engineering an der Universität Potsdam. Can be accessed at: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10314/file/tbhpi113.pdf (as at 19.10.2018).

MEISSER, CHRISTIAN / MEISSER, LUZIUS / KOGENS, RONALD (2018): Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs. In: Jusletter IT of 24 May 2018.

MERCIER, GREGOR (2016): Art. 84 OR. In: Amstutz, Marc / Breitschmid, Peter / Furrer, Andreas / Girsberger, Daniel / Huguenin, Claire / Jungo, Alexandra / Müller-Chen, Markus / Roberto, Vito / Schnyder, Anton K. Z/ Trüeb, Hans Rudolf (eds.): Handkommentar zum Schweizer Privatrecht. 3th edition. Zurich, Schulthess.

MEYER, STEPHAN D. / SCHLUPPI, BENEDIKT (2017): "Smart Contracts" und deren Einordnung in das schweizerische Vertragsrecht. In: recht 2017/3, 204–224.

MÖSER, MALTE / SOSKA, KYLE / HEILMAN, ETHAN / LEE, KEVIN / HEFFAN, HENRY / SRIVASTAVA, SHASHVAT (2018): An Empirical Analysis of Traceability in the Monero Blockchain. Can be accessed at: https://arxiv.org/pdf/1704.04299/ (as at 11.10.2018).

MÜLLER, LUKAS / REUTLINGER, MILENA / KAISER, PHILIPPE J.A. (2018): Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union. In: EuZ 2018/3, 80–102.

MÜLLER, LUKAS / STOLTZ, THOMAS / KALLENBACH, TOBIAS A. (2017): Liberierung des Aktienkapitals mittels Kryptowährung. In: AJP 2017/11, 1318–1333.

MÜLLER, THOMAS S. (2013): Einleitung. In: Watter, Rolf / Vogt, Nedim Peter / Bauer, Thomas / Winzeler, Christoph (eds.): Basler Kommentar zum Bankengesetz. Basel: Helbing Lichtenhahn.

MÜLLER-CHEN MARKUS (2018): Art. 105 IPRG. In: Müller-Chen, Markus / Widmer Lüchinger, Corinne (eds.): Zürcher Kommentar IPRG. 3rd edition. Zurich: Schulthess.

NAKAMOTO, SATOSHI (2018): Bitcoin: A Peer-to-Peer Electronic Cash System. Can be accessed at: https://bitcoin.org/bitcoin.pdf (as at 19.10.2018).

NARAYAN, ARVIND / BONNEAU, JOSEPH / FELTEN, EDWARD / MILLER, ANDREW / GOLDFEDER, STEVEN (2016): Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press.

NEUENSCHWANDER, PETER K. / OESCHGER, SIMON (2017): Daten im Konkurs: Herausforderungen in der Praxis. In: Jusletter IT of 11 December 2017.

OFTINGER, KARL / BÄR, ROLF (1981): Das Fahrnispfand Art. 884-918 ZGB. Zürcher Kommentar. 3rd edition. Zurich: Schulthess.

PETITPIERRE-SAUVAIN, ANNE (2006): Les papiers-valeurs. Schweizerisches Privatrecht Band VIII/7. Basel: Helbing Lichtenhahn.

PILLER, FRANCOIS (2017): Virtuelle Währungen – Reale Rechtsprobleme? In: AJP 2017/12, 1426–1438.

PÖSCHEL, INES / MAIZAR, KARIM (2012): Art. 973*c* OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar Wertpapierrecht. Basel: Helbing Lichtenhahn.

PULVER, URS / SCHOTT, BERTRAND (2011): Das Insolvenzrecht für Banken und Effektenhändler – Überblick über die Sonderregelung und ausgewählte Fragen. In:

Sprecher, Thomas (ed.): Sanierung und Insolvenz von Unternehmen. Zurich: Schulthess, 237–291.

RAYROUX, FRANÇOIS / DU PASQUIER, SHELBY (2016): Art. 7 KAG. In: Bösch, René / Rayroux, François / Winzeler, Christoph / Stupp, Eric (eds.): Basler Kommentar Kollektivanlagengesetz. Basel: Helbing Lichtenhahn.

REISER, NINA (2018): Ist der Bankbegriff im Lichte aktueller technologischer Entwicklungen noch zeitgemäss? In: AJP 2018/7, 811–824.

REUTTER, THOMAS / RAUN, DANIEL (2018): Insider Trading and Market Manipulation in Tokens, CapLaw 2018/4, 4–7.

REUTTER, THOMAS / STEINMANN, CHRISTIAN (2012): Vor Art. 1157-1186 OR. In: Honsell, Heinrich / Vogt, Nedim Peter / Watter, Rolf (eds.): Basler Kommentar Wertpapierrecht. Basel: Helbing Lichtenhahn.

REY, HEINZ (2007): Die Grundlagen des Sachenrechts und das Eigentum. 3rd edition. Bern: Stämpfli.

RUSSENBERGER, MARC (2010): Art. 242 SchKG. In: Staehelin, Adrian / Bauer, Thomas / Staehelin, Daniel (eds.): Basler Kommentar Bundesgesetz über Schuldbetreibung und Konkurs. 2nd edition. Basel: Helbing Lichtenhahn.

SCHMID, JÖRG / HÜRLIMANN-KAUP, BETTINA (2017): Sachenrecht. 5th edition. Zurich: Schulthess.

SCHOBER, ROGER /AVDYLI-LUGINBÜHL, MONIKA (2017): Art. 242 SchKG. In: Kren Kostkiewicz, Jolanta / Vock, Dominic (eds.): Kommentar zum Bundesgesetz über Schuldeintreibung und Konkurs SchKG. Zurich: Schulthess.

SCHOLL, MARCEL (2018): Vermögenseinziehung (Art. 70 StGB). In: Ackermann, Jürg-Beat (ed.): Kommentar Kriminelle Vermögen, Kriminelle Organisationen, Volume II. Zurich: Schulthess, 259–578.

SCHÖNKNECHT, FLORIAN (2016): Der Einlagebegriff nach Bankengesetz. In: GesKR 2016/3, 300–319.

SCHOTT, ANSGAR / WINKLER, MARKUS (2017): Art. 26 FinfraG. In: Sethe, Rolf / Favre, Olivier / Hess, Martin / Kramer, Stefan / Schott, Ansgar (eds.): Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG. Zurich: Schulthess.

SCHWENZER, INGEBORG (2016): Schweizerisches Obligationenrecht, Allgemeiner Teil. 7th edition. Bern: Stämpfli.

SCORER, SIMON (2017): Central Bank Digital Currency: DLT, or not DLT? That is the question. Can be accessed at: https://bankunderground.co.uk/2017/06/05/central-bank-digital-currency-dlt-or-not-dlt-that-is-the-question/ (as at 19.10.2018).

SEILER, BENEDIKT / SEILER, DANIEL (2018): Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH) und Ripple (XRP) als Sachen im Sinne des ZGB zu behandeln? In: sui-generis 2018, 149–163.

SIMMLER, MONIKA / SELMAN, SINE / BURGERMEISTER, DANIEL (2018): Beschlagnahme von Kryptowährungen im Strafverfahren. In: AJP 2018/8, 963–978.

SPIRIG, EUGEN (1993): Die Abtretung von Forderungen und die Schuldübernahme. Zürcher Kommentar. 3rd edition. Zurich: Schulthess.

STENGEL, CORNELIA / AUS DER AU, ROMAN (2018): Blockchain: Eine Technologie für effektiven Datenschutz? In: sic! 2018/9, 439–452.

STRATENWERTH, GÜNTER (2000): Schweizerisches Strafrecht, Besonderer Teil II: Straftaten gegen Gemeininteressen. 5th edition. Bern: Stämpfli.

SZABO, NICK (1996): Smart Contracts: Building Blocks for Digital Markets. Can be accessed at: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (as at 19.10.2018).

SZABO, NICK (1997): Formalizing and Securing Relationships on Public Networks. Can be accessed at: https://nakamotoinstitute.org/formalizing-securing-relationships/ (as at 19.10.2018).

TAUBE, TAMARA (2013): Entstehung, Bedeutung und Umfang der Sorgfaltsplfichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag. Zurich / St.Gallen: Dike.

THOUVENIN, FLORENT (2017): Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs. In: SJZ 2017/113, 21–32.

THOUVENIN, FLORENT / FRÜH, ALFRED / LOMBARD, ALEXANDRE (2017): Eigentum an Sachdaten: Eine Standortbestimmung. In: SZW 2017/1, 25–34.

THOUVENIN, FLORENT / WEBER, ROLF H. (2017): Zum Bedarf nach einem Dateneigentum. In: Jusletter IT of 11 December 2017.

TRÜEB, HANS RUDOLF (2018): Smart Contracts. In: Grolimund, Pascal / Koller, Alfred / Loacker, Leander D. / Portmann, Wolfgang (eds.): Festschrift für Anton K. Schnyder. Zurich: Schulthess, 723-734.

TRUFFER, ROLAND (2011): Art. 7 BEHG. In: Vogt, Nedim Peter / Watter, Rolf (eds): Basler Kommentar Börsengesetz / Finanzmarktaufsichtsgesetz. 2nd edition. Basel: Helbing Lichtenhahn.

VISCHER, FRANK (2004): Art. 151 IPRG. In: Girsberger, Daniel / Heini, Anton / Keller, Max / Kren Kostkiewicz, Jolanta / Siehr, Kurt / Vischer, Frank / Volken, Paul (eds.): Zürcher Kommentar zum IPRG. 2nd edition. Zurich: Schulthess.

VISCHER, FRANK / WEIBEL, THOMAS (2018): Art. 155 IPRG. In: Müller-Chen, Markus / Widmer Lüchinger, Corinne (eds.): Zürcher Kommentar IPRG. 3rd edition. Zurich: Schulthess.

VON DER CRONE, HANS CASPAR / KESSLER, FRANZ J. / ANGSTMANN, LUCA (2018): Token in der Blockchain – privatrechtliche Aspekte der Distributed Ledger Technologie. In: SJZ 2018/14, 337–345.

WATTER, ROLF / ROTH PELLANDA, KATJA (2013): Art. 156 IPRG. In: Honsell, Heinrich / Vogt, Nedim Peter / Schnyder, Anton K. / Berti, Stephen V. (eds.): Basler Kommentar Internationales Privatrecht. 3rd edition. Basel: Helbing Lichtenhahn.

WEBER, LAURENCE / TAKACS, ALEXANDRE (2018): Le bitcoin : ce qu'il faut savoir sur le plan juridique. In: Plädoyer 2018/2, 37 ff.

WEBER, ROLF H. (2018): Smart Contracts: Vertrags- und verfügungsrechtlicher Regelungsbedarf? In: sic! 2018/6, 291–301.

WEBER, ROLF H. (2017): Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts: Eine Auslegeordnung möglicher Problemstellungen. In: Jusletter of 4 December 2017.

WEBER, ROLF H. (2015): Überblick über die rechtlichen Rahmenbedingungen für webbasierte und mobile Zahlungssysteme. In: Weber, Rolf H. / Thouvenin, Florent (eds.): Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme. Zurich: Schulthess, 5–38.

WEBER, ROLF H. (2005): Art. 84 OR. Berner Kommentar – OR Allgemeine Bestimmungen (Art. 68-96 OR). 2. Aufl. Bern: Stämpfli.

WEBER, ROLF H. (1998): Juristische Personen. Schweizerisches Privatrecht Volume II/4. Basel: Helbing Lichtenhahn.

WEBER, ROLF H. / IACANGELO, SALVATORE (2018): Rechtsfragen bei der Übertragung von Token. In: Jusletter IT of 24 May 2018.

WEBER, ROLF H. / THOUVENIN, FLORENT (2018): Dateneigentum und Datenzugangsrechte – Bausteine der Informationsgesellschaft? In: ZSR 2018/1, 43–74.

WIATROWSKI, ALEKSANDER (2018): Blockchain Technology – a Threat or a Solution for Data Protection? In: Jusletter IT of 22 February 2018.

WILE, ROB (2014): Supporter of Extremist Group ISIS Explains How Bitcoin Could be Used to Fund Jihad. In: Business Insider Australia. Can be accessed at: https://www.businessinsider.com.au/isis-supporter-outlines-how-to-support-terror-group-with-bitcoin-2014-7 (as at 19.10.2018).

ZANOL, JAKOB / CZADILEK, ALEXANDER / LEBLOCH, KASPAR (2018): Self-Sovereign Identity und Blockchain. In: Jusletter IT of 22 February 2018.

ZELLWEGER GUTKNECHT CORINNE (2018): Developing the Right Regulatory Regime for Cryptocurrencies and Other Value Data, in: Fox David / Green Sarah (eds.). Private and Public Law Implications of Cryptocurrencies, in print, can be accessed at: http://ssrn.com/abstract=3240454 (as at 12.11.2018).

ZETSCHE, DIRK A. / ROSS, P. BUCKLEY / DOUGLAS, ARNER W. / FÖHR, LINUS (2017): THE ICO Gold Rush: It's a Scam, it's a Bubble, it's a Super Challenge for Regulators. Can be accessed at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298 (as at 19.10.2018).

ZOBL, DIETER (2001): Internationale Übertragung und Verwahrung von Wertpapieren (aus Schweizer Sicht). In: SZW 2001, 105–121.

ZOBL, DIETER / GERICKE, DIETER (2013): Systematischer Teil des BEG. In: Zobl, Dieter / Hess, Martin / Schott, Ansgar (eds.): Kommentar zum Bucheffektengesetz (BEG). Zurich: Schulthess.

9.2 List of materials

Blockchain Taskforce 2018a	Blockchain Taskforce, Strengthening the blockchain in Switzerland, The White Paper of the Blockchain Taskforce, April 2018. Available at: www.blockchaintaskforce.ch (as at 18 October 2018)
Blockchain Taskforce 2018b	Blockchain Taskforce, Position Paper on the Legal Classification of ICOs, April 2018. Available at: www.blockchaintaskforce.ch (as at 18 October 2018)
CGMF 2018a	Interdepartemental coordinating group on combating money laundering and the financing of terrorism, Risk of money laundering and financing of terrorism by crypto assets and crowdfunding, dated October 2018. Available at: www.admin.ch > Documentation > Media releases > Press release of 14 December 2018 (as at 14 December 2018).
CGMF 2018b	Interdepartemental coordinating group on combating money laundering and the financing of terrorism, Report on the use of cash and its risks of abuse for money laundering and financing of terrorism in Switzerland, of October 2018. Publication expected on 18 December 2018. After publication, available at: www.admin.ch > Documentation > Media releases > Press release of 18 December 2018.
CNIL 2018	Commission Nationale Informatique & Libertés, Premier éléments d'analyse de la CNIL, Blockchain, September 2018. Available at: www.cnil.fr > Technologies > Blockchain (as at 19 October 2018).
CPMI 2015	Committee on Payments and Market Infrastructures, Report of 23 November 2015 on Digital Currencies (CPMI Papers No. 137). Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018)
CPMI 2016	Committee on Payments and Market Infrastructures, Report of 8 November 2016 on Fast payments – Enhancing the speed and availability of retail payments (CPMI Report No. 154). Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018).
CPMI 2017	Committee on Payments and Market Infrastructures, Report of 27 February 2017 on Distributed ledger technology in payment, clearing and settlement – an analytical framework (CPMI Paper No. 157). Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018).
CPMI 2018a	Committee on Payments and Market Infrastructures, Report of 16 February 2018 on Cross-border retail payments (CPMI Paper No. 173). Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018).

CPMI 2018b	Committee on Payments and Market Infrastructures, Report of 12 March 2018 on Central bank digital currencies (CPMI Paper No. 174). Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018).
CPMI/IOSCO 2012	Committee on Payment and Settlement Systems / International Organization of Securities Commissions, Principles for financial market infrastructures, April 2012. Available at: www.bis.org > Committees & associations > Committee on Payments and Market Infrastructures > Publications (as at 18 October 2018).
Deutsche Bundesbank 2017	Deutsche Bundesbank, Monatsberichtsaufsatz vom September 2017, Distributed-Ledger-Technologien im Zahlungsverkehr und der Wertpapierabwicklung: Potenziale und Risiken. Available at: www.bundesbank.de > Publikationen > Berichte und Studien (as at 18 October 2018).
Dispatch regarding AMLA	Dispatch of 17 June 1996 on the Federal Act on Combating Money Laundering in the Financial Sector (Anti-Money Laundering Act, AMLA), in: BBl **1996** III 1101
Dispatch regarding FinSA/FinIA	Dispatch of 4 November 2015 on the Financial Services Act (FinSA) and the Financial Institutions Act (FinIA), in: BBl **2015** 8901
Dispatch regarding FISA	Dispatch of 15 November 2006 on the Federal Intermediated Securities Act and the Hague Securities Convention, in: BBl **2006** 9315
Dispatch regarding FMIA	Dispatch of 3 September 2014 on the Financial Market Infrastructure Act (FMIA), in: BBl **2014** 7483
Dispatch regarding SESTA	Dispatch of 24 February 1993 on a Federal Act on Stock Exchanges and Securities Trading, in BBl **1993** Vol. I 1369
European Parliament 2018	European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Study on Virtual currencies and terrorist financing: assessing the risks and evaluating responses, May 2018. Available at: www.europarl.europa.eu > Other websites > Think Tank (as at 19 October 2018)
FDF Explanatory Report FinSO/FinIO 2018	Federal Department of Finance FDF, Report on the FinSO/FinIO consultation draft of 24 October 2018. Available at: www.admin.ch > Documentation > Media releases (Press release of 24 October 2018) (as at 14 November 2018).
FDF Explanatory Report Fintech 2017a	Federal Department of Finance FDF, Explanatory report on amendments to the Banking Act and Banking Ordinance (fintech), Explanatory report on the consultation draft, 1 February 2017. Available at: www.admin.ch > Documentation > Media releases (Press release of 1 February 2017) (as at 19 October 2018).
FDF Explanatory Report Fintech 2017b	Federal Department of Finance FDF, Report on amendments to the Banking Ordinance (Fintech), Explanations, 5 July 2017. Available at: www.admin.ch > Documentation > Media releases (Press release of 5 July 2017) (as at 19 October 2018).

FDF Explanatory Report FMIO 2015	Federal Department of Finance FDF, Explanatory report on the Ordinance on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading, 25 November 2015. Available at: www.admin.ch > Documentation > Media releases (Press release of 25 November 2015) (as at 19 October 2018).
FDF Explanatory Report AMLO 2015	Federal Department of Finance FDF, Explanatory report on the Anti-Money Laundering Ordinance (AMLO) – Implementation of FATF Recommendations, 11 November 2015. Available at: www.admin.ch > Documentation > Media releases (Press release of 11 November 2015) (as at 19 October 2018).
FINMA 2017	Swiss Financial Market Supervisory Authority FINMA, FINMA Guidance 04/2017, Regulatory treatment of initial coin offerings, 29 September 2017. Available at: www.finma.ch > Documentation > FINMA Guidance (as at 19 October 2018).
FINMA 2018a	Swiss Financial Market Supervisory Authority FINMA, ICO Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs), updated 16 February 2018. Available at: www.finma.ch > Authorisation > Fintech (as at 19 October 2018).
FINMA 2018b	Swiss Financial Market Supervisory Authority FINMA, Fact sheet: "Virtual Currencies", updated 30 August 2018. Available at: www.finma.ch > Documentation > FINMA publications > Fact sheets (as at 19 October 2018).
FINMA Circ. 2018/2	Swiss Financial Market Supervisory Authority FINMA, FINMA Circular 2018/2 (Duty to report securities transactions), updated 1 January 2018. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).
FINMA Circ. 2018/1	Swiss Financial Market Supervisory Authority FINMA, FINMA Circular 2018/1 (Organised trading facilities), updated 1 January 2018. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).
FINMA Circ. 2013/8	Swiss Financial Market Supervisory Authority FINMA, FINMA Circular 2013/8 (Market conduct rules), updated 12 August 2016. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).
FINMA Circ. 2011/1	Swiss Financial Market Supervisory Authority FINMA, Rundschreiben 2011/1 (Tätigkeit als Finanzintermediär nach GwG), updated 26 October 2016. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).
FINMA Circ. 2008/5	Swiss Financial Market Supervisory Authority FINMA, Rundschreiben 2008/5 (Effektenhändler), updated 12 August 2016. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).
FINMA Circ. 2008/3	Swiss Financial Market Supervisory Authority FINMA, Rundschreiben 2008/3 (Publikumseinlagen bei Nichtbanken), updated 7 December 2017. Available at: www.finma.ch > Documentation > Circulars (as at 19 October 2018).

FSB 2018	Financial Stability Board (FSB), Crypto-asset markets: Potential channels for future financial stability implications, October 2018. Available at: www.fsb.org > Publications > Browse All Publications (as at 19 October 2018).
IMF 2018a	International Monetary Fund, Finance & Development, Money, Transformed: The future of currency in a digital world, June 2018. Available at: www.imf.org > Publications > Finance & Development (as at 18 October 2018).
IMF 2018b	International Monetary Fund, World Economic Outlook, October 2018. Available at: www.imf.org > Publications > World Economic Outlook (as at 18 October 2018).
Report on Virtual Currencies	Federal Council report of 25 June 2014 on virtual currencies in response to the Schwaab (13.3687) and Weibel (13.4070) postulates. Available at: www.admin.ch > Documentation > Media releases (Press release of 25 June 2014) (as at 18 October 2018)
SNB 2018	Swiss National Bank: Survey on payment methods 2017, Survey on payment methods and use of cash in Switzerland, dated May 2018. Available at: www.snb.ch > Banknotes and coins > Survey on payment methods (as at 18 October 2018).

9.3 Abbreviations

AJP	Aktuelle Juristische Praxis
AMLA	Federal Act of 10 October 1997 on Combating Money Laundering and the Financing of Terrorism in the Financial Sector (Anti-Money Laundering Act; SR *955.0*)
AMLO	Ordinance of 11 November 2015 on Combating Money Laundering and Terrorist Financing (Anti-Money Laundering Ordinance; SR *955.01*)
AMLO-FINMA	Ordinance of the Swiss Financial Market Supervisory Authority of 3 June 2015 on the Prevention of Money Laundering and the Financing of Terrorism (FINMA Anti-Money Laundering Ordinance; SR *955.033.0*)
Art.	article
BankA	Federal Act of 8 November 1934 on Banks and Savings Banks (Banking Act; SR *952.0*)
BankO	Ordinance of 30 April 2014 on Banks and Savings Banks (Banking Ordinance, SR *952.02*)
BBl	Federal Gazette (www.admin.ch > Bundesrecht > Bundesblatt)
BCBS	Basel Committee on Banking Supervision (www.bis.org/bcbs)
BIS	Bank for International Settlements (www.bis.org)
BTC	Bitcoin
CC	Swiss Civil Code of 10 December 1907 (SR *210*)
CGMF	Coordinating group on combating money laundering and the financing of terrorism
CHF	Swiss franc
CISA	Federal Act of 23 June 2006 on Collective Capital Investment Schemes (Collective Investment Schemes Act, SR *951.31*)
CISO	Ordinance of 22 November 2006 on Collective Investment Schemes (Collective Investment Schemes Ordinance, SR *951.311*)
CO	Federal Act of 30 March 1911 on the Amendment of the Swiss Civil Code (Part Five: The Code of Obligations; SR *220*)
CPC	Swiss Civil Procedure Code of 19 December 2008 (SR *272*)
CPIA	Federal Act of 22 December 1999 on Currency and Payment Instruments (SR *941.10*)
CPMI	Committee on Payments and Market Infrastructures (www.bis.org/cpmi)
CR	Computer und Recht
CRO	Commercial Register Ordinance of 17 October 2007 (SR *221.411*)
DAO	decentralised autonomous organisation
DApps	decentralised applications

DEBA	Federal Act of 11 April 1889 on Debt Enforcement and Bankruptcy (SR *281.1*)
DLT	distributed ledger technology
DUFI	financial intermediary directly subordinated
E-ID	electronic identification
ERC20	Ethereum Request for Comment-20
ESigA	Federal Act of 18 March 2016 on Certification Services in relation to Electronic Signatures (Federal Act on Electronic Signatures, SR *943.03*)
ETH	Ether
EuZ	Zeitschrift für Europarecht
FATF	Financial Action Task Force (www.fatf-gafi.org)
FDF	Federal Department of Finance
FinIA	Federal Act of 15 June 2018 on Financial Institutions (Financial Institutions Act, BBl *2018* 3557)
FinIO	Ordinance on Financial Institutions (Financial Institutions Ordinance, *not yet adopted*)
FINMA	Swiss Financial Market Supervisory Authority (www.finma.ch)
FINMA Circ.	FINMA Circular
FINMASA	Federal Act of 22 June 2007 on Federal Financial Market Supervision (Financial Market Supervision Act, SR *956.1*)
FinSA	Federal Act of 15 June 2018 on Financial Services (Financial Services Act; BBl *2018* 3615)
FinSO	Ordinance on Financial Services (Financial Services Ordinance, *not yet adopted*)
FISA	Federal Act of 3 October 2008 on Intermediated Securities (Federal Intermediated Securities Act; SR *957.1*)
FMI(s)	financial market infrastructure(s)
FMIA	Federal Act of 19 June 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Act; SR *958.1*)
FMIO	Ordinance of 25 November 2015 on Financial Market Infrastructures and Market Conduct in Securities and Derivatives Trading (Financial Market Infrastructure Ordinance; SR *958.11*)
FOJ	Federal Office of Justice
FSB	Financial Stability Board (www.fsb.org)
GBP	pound sterling
GesKR	Zeitschrift für Gesellschafts- und Kapitalmarktrecht
ICO	initial coin offering

IMF	International Monetary Fund (www.imf.org)
IOA	Federal Act of 17 December 2004 on the Oversight of Insurance Companies (Insurance Oversight Act, SR *961.01*)
IOSCO	International Organization of Securities Commissions (www.iosco.org)
IoT	internet of things
IPA	Federal Act of 2 April 1908 on Insurance Policies (Insurance Policies Act, SR *221.229.1*)
ISO	International Organization for Standardization
KID	Key Information Document
KYC	know your customer
let.	letter(s)
LPCCI	limited partnership for collective capital investments
L-QIF	limited qualified investment funds
LugC	Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters done at Lugano on 30 October 2007 (Lugano Convention, SR *0.275.12*)
margin no.	margin number(s)
MROS	Money Laundering Reporting Office Switzerland
MTF	multilateral trading facility
n.	note(s)
NBA	Federal Act on the Swiss National Bank of 3 October 2003 (National Bank Act, SR *951.11*)
NBO	Ordinance on the Federal Act on the Swiss National Bank of 18 March 2004 (National Bank Ordinance, SR *951.131*)
NJW	Neue Juristische Wochenschrift
OECD	Organisation for Economic Co-operation and Development (www.oecd.org)
OTC	over-the-counter
OTF	organised trading facility
para.	paragraph
PILA	Federal Act of 18 December 1987 on Private International Law (SR *291*)
RTGS	real time gross settlement
SBA	Swiss Bankers Association
SCC	Swiss Criminal Code of 21 December 1937 (SR *311.0*)
SEC	Securities and Exchange Commission (www.sec.gov)
SECOM	securities settlement system of SIX Group

SESTA	Federal Act of 24 March 1995 on Stock Exchanges and Securities Trading (Stock Exchange Act; SR *954.1*)
SESTO	Ordinance of 2 December 1996 on Stock Exchanges and Securities Trading (Stock Exchange Ordinance, SR *954.11*)
SIC	Swiss Interbank Clearing
SICAF	investment company with fixed capital
SICAV	investment company with variable capital
SJZ	Schweizerische Juristen-Zeitung
SNB	Swiss National Bank (www.snb.ch)
SR	Classified Compilation of Federal Legislation
SRO	self-regulatory organisation
SZW	Schweizerische Zeitschrift für Wirtschafts- und Finanzmarktrecht
UNCITRAL	UN Commission on International Trade Law
USC	Utility Settlement Coin
USD	US dollar
VASP	virtual asset service provider
ZSR	Zeitschrift für Schweizerisches Recht