SwissBanking

August 2019, 2nd edition

SBA guidelines on opening corporate accounts for DLT companies

Content

Foreword

The number of distributed ledger technology (DLT) companies in Switzerland has increased markedly over recent years. The Swiss Bankers Association (SBA) welcomes this trend and takes a positive view of the high market momentum, as it boosts Switzerland's attractiveness as a workplace and financial centre. Banks see blockchain technology as an opportunity that opens up an array of possibilities for the country as a financial and technology location.

With the growth of DLT companies, their demand for corporate accounts with banks in Switzerland has also risen. While technological advances do not in themselves constitute a particular risk and are essentially neutral, opening an account poses various challenges for banks because DLT-specific applications can also be associated with risks, especially in relation to money laundering in the use of cryptocurrencies, or fraud. Switzerland has strict laws and due diligence requirements in place governing financial transactions. Banks must therefore carry out careful checks when opening an account.

Under the aegis of the SBA, a working group has revised the terminology and content of the 2018 guidelines on opening corporate accounts for blockchain companies. These guidelines are intended to support member banks in their discussions with such companies, and at the same time assist with risk management in their business dealings. The Federal Department of Finance (FDF) and FINMA welcome the publication of these guidelines. The Crypto Valley Association (CVA) also helped to revise the guidelines and supports their implementation in practice.

1. Background and structure of the guidelines

The guidelines address potential requirements that a bank may place on a company involved with distributed ledger technology (DLT) when opening a corporate account. The potential requirements to some extent exceed the applicable minimum legal obligations of companies involved with DLT, but they are not intended to replace applicable rules or existing official guidelines.

The guidelines are based on the principle that the regulations on combating money laundering and terrorist financing, like all other horizontal regulations, are also applicable to all participating financial intermediaries in the area of DLT. The AML duties of a bank that apply generally when opening a corporate account are therefore based on the valid version of the Agreement on the Swiss banks' code of conduct with regard to the exercise of due diligence (CDB), AMLO-FINMA, AMLA and the Swiss Criminal Code, in addition to bank-specific internal guidelines. These guidelines build on the CDB and also cover DLT-related issues. As far as possible, the recommendations published by the Financial Action Task Force (FATF) in June 2019 were taken into account when drafting this version. The guidelines will be updated as necessary in response to further developments.

The guidelines are intended to reflect the differing nature and dynamics of companies involved with DLT. Depending on the maturity and business-specific strategy of the company, not all of the recommendations are relevant to account opening or ongoing account maintenance. For example, a traditionally financed start-up can apply for a corporate account in its initial phase and only arrange for the issuing of tokens one to two years later. Furthermore, long-standing corporate clients can decide to offer blockchain services, accept cryptocurrencies as a payment method or issue tokens for the first time. The latter may even include companies whose business models have no involvement with DLT but which want to finance themselves via that channel.

Therefore, the guidelines address DLT-specific elements within the scope of the established KYC process and contain specific expectations for the issuers of tokens. Consequently, the guidelines differentiate between companies with general involvement with DLT and companies with involvement in activities relevant to AML, in particular cryptoassets and the issuing of tokens.

When it comes to issuing tokens, the guidelines further differentiate between financing with cryptocurrencies (usually Bitcoin or Ethereum) and financing with government currencies (fiat money).

The guidelines only cover token issues that are carried out by an operating company domiciled in Switzerland and that are governed by the FINMA guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) dated 16 February 2018. In case of a connection to foreign countries, e.g. when participants in a token issue and other involved parties are domiciled abroad, the risks resulting from the application of foreign regulations (tax law, criminal law, anti-money laundering law, capital market law, etc.) must be adequately captured, limited and controlled.

The current version of the guidelines does not cover the maintenance of cryptoasset accounts for clients.

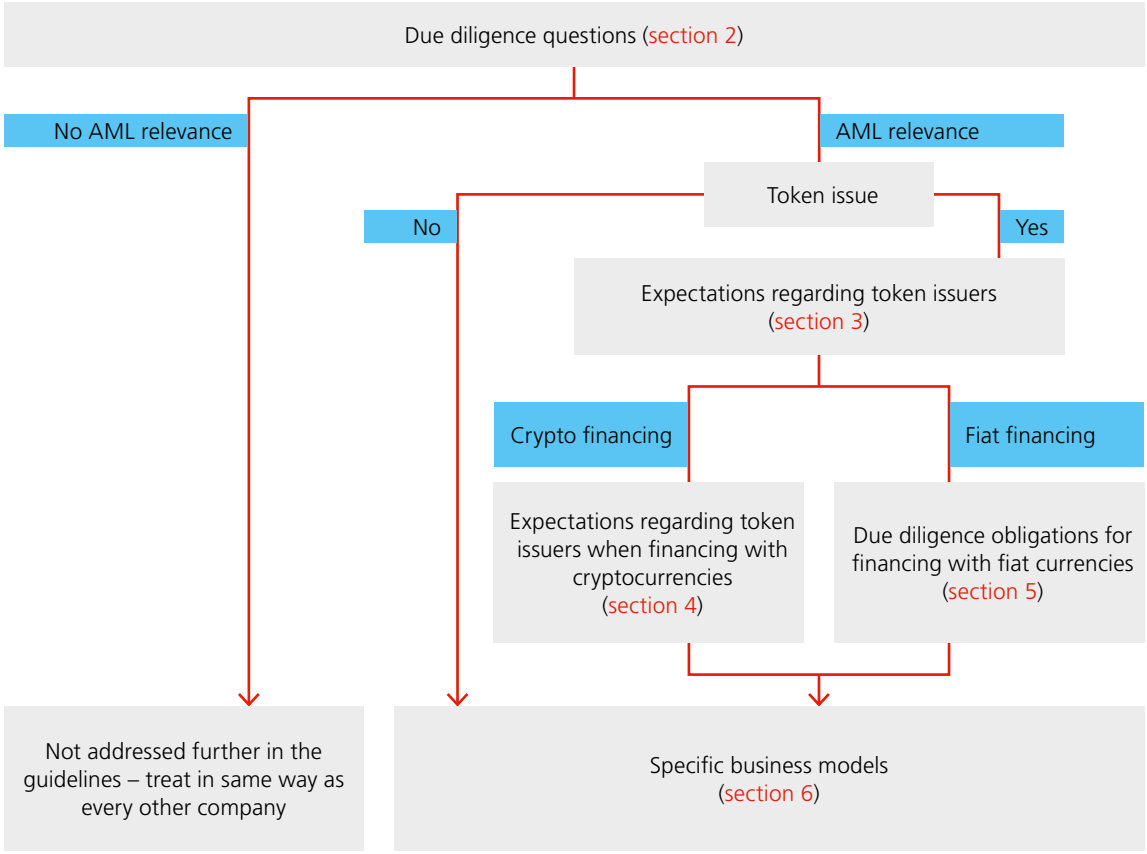
The guidelines only pertain to members of the SBA. Internal instructions issued by SBA members always take precedence. The guidelines do not set any industry-wide minimum standards. Each individual institution may interpret and apply the guidelines within the scope of its own internal risk appetite.

There is no legal obligation on the part of SBA members to open accounts.

The guidelines are periodically updated and expanded.

Fig. 1

Structure of the guidelines



Source: SBA

2. Due diligence questions for corporate clients involved with DLT

This section covers the specific expectations within the scope of the KYC process that result from general involvement with DLT (with or without token issuance).

It is recommended that the documents and materials listed below be obtained from corporate clients prior to opening any accounts. The comments below also include the conversion of a blocked account into a business account for operational purposes during a company foundation.

Measure / check	Recommendation
2.1 DLT involvement	Specific description of the areas of involvement
2.2 Description of the business model	• Conclusive and comprehensible description based on reliable-documentation such as a white paper • Description of the expected payment flows • Description of the planned operational set-up • In national/business language • Identification of the legal form • Description of any smart contracts including independent audit review for existing tokens as additional risk mitigation
2.3 Exclusion of domiciliary companies	• The company should demonstrate that it is operational (CDB 16) and has a local presence. • When setting up a new company: the company should disclose its intentions, purpose and expected current revenue and expenses.
2.4 Regulatory competencies	The company should have a dedicated contact for all compliance and regulatory issues. In particular it should have: • knowledge of the relevant rules/regulations • a description of how the company implements the relevant rules (internal guidelines).
2.5 Validation of the business model after account opening	Account holders are obliged to notify the bank of any relevant change in their use of blockchain technology or an upcoming token issue.
2.6 Triage	• If the company has no specific involvement with DLT that is relevant to AML (token issuance, cryptoassets): account opening should be conducted in accordance with internal guidelines, as for other companies. • If the company is planning to issue tokens within the next 12 months: go to section 3 (General expectations regarding token issuers). • If the company is not issuing tokens but has involvement with DLT that is relevant to AML: go to section 6 (Specific business models).

Companies that issued tokens previously and prior to commencement of the account relationship must, on request, supply complete documentation of the KYC / AML process as per section 3 and section 4 and demonstrate that they comply with Swiss regulations.

3. General expectations regarding token issuers

This section addresses the issuing of tokens, often also referred to as a token-generating event (TGE), regardless of the type of financing. It only discusses token issues by operating companies domiciled in Switzerland.

The utmost priority is placed on preserving the reputation and the integrity of Switzerland as a financial centre and workplace. The recommendations in section 3 and section 4 are based on this overriding objective and also serve to protect the token issuer.

An account can be opened as described in section 2 before the measures and checks for token issues described in section 3 have been carried out. A traditional corporate account can then be upgraded to a "DLT account" (for example to receive funds as part of a token issue and/or for specific business models as described in section 6), provided the due diligence obligations set out in the following sections are complied with. If the previously used corporate account is also used when financing and issuing tokens, the bank must put in place operational measures to ensure that the funds arising out of the token issue can only be deposited in the corporate account once a full check has been carried out.

The bank should not conduct any legal analysis of the nature and maturity of the tokens and should initially assume that the issuer is subject to the AMLA. If it is not subject to the AMLA, the token issuer must state this and explain the reasons why. In case of doubt, it must in particular produce proof in the form of an ICO enquiry answered by FINMA. The AMLA stipulates various due diligence obligations and the duty to either join a self-regulatory organisation (SRO) or allow a Swiss financial intermediary subject to the AMLA to receive its assets.

Institution-specific internal instructions may set additional requirements. Internal instructions always take precedence over the guidelines.

Measure / check	Recommendation
3.1 Description (Token)	• Detailed description of the tokens to be issued in accordance with the appendix to the FINMA guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) dated 16 February 2018 and the stage of development (market maturity, issue date) • The token issuers should, prior to the issue, demonstrate that the project to be financed exists and that the funds deposited in the account are derived from the token issue and are subsequently to be used for the stated purpose. • The token documentation, mostly in the form of a white paper, is an essential component of the bank's due diligence. It should therefore be submitted to the bank at which the account is held as soon as possible. • When issuing tokens, the issuer should disclose the method of operation and the data linked to the DLT application. • Independent technical audit review of any smart contract as an additional risk mitigation measure
3.2 Liquidity planning	The token issuer should notify the bank at which the account is held prior to the token issue of the following: • the expected breakdown of fiat money and individual cryptocurrencies (e.g. 50 % fiat, 25 % Bitcoin, 25 % Ethereum) • the amounts and frequency at which the funds converted into fiat money will be transferred to the bank at which the account is held • repayment schedule if the target amount is not reached (including the relevant contractual clause) • the companies at which the cryptocurrencies are exchanged (section 4.7)
3.3 Handling risks under foreign law	A token issuer must have appropriate guidelines in place and must implement measures to exclude investors from countries in accordance with the bank's internal definition. When issuing tokens as part of a security token offering (STO), the issuer should supply the bank at which the account is held with a list of the target countries, demonstrating that the corresponding local regulations are complied with at all times. The token issuer should supply this information to the bank on request.

3.4 Applicability of AMLA	The bank should initially assume that the token issuer is subject to the AMLA. Applicability of the AMLA is exclusively based on the FINMA guidelines for ICOs dated 16 February 2018. If the token issuer is not subject to the AMLA, it must demonstrate this. In case of doubt, it must in particular produce an ICO enquiry answered by FINMA. If subject to the AMLA, the token issuer should produce the following documentary evidence: • name of the SRO and confirmation of SRO membership or • in case of delegation: name of the financial intermediary, confirmation of its membership of an SRO and confirmation of delegation • complete documentation in accordance with the internal compliance rules of the bank at which the account is held
3.5 Duties after issue	• Legal obligations are based on the AMLA. • At the bank's request, the issuer should demonstrate to the bank that the current use of funds corresponds with the stated purpose. • At the bank's request, the issuer should demonstrate to the bank that the restrictions for foreign investors described in section 3.3 have been complied with. • As a rule, any measure to create transparency with regard to the change of (token) ownership after the completion of the issue mitigates risk and is welcomed by the bank at which the account is held. This includes the submission of corresponding information, where available, at the request of the bank at which the account is held. • Where the business model involves AMLA-relevant activities, membership of an SRO is mandatory.
3.6 Financing type triage	• If the token issuer arranges for some or all of the financing on blockchain/via a cryptocurrency: go to section 4 (Expectations regarding token issuers when financing with cryptocurrencies). • If the financing is carried out exclusively with fiat money: go to section 5 (Due diligence obligations for financing with fiat currencies).

4. Expectations regarding token issuers when financing with cryptocurrencies

This section describes corporate financing that is partially or entirely executed through cryptocurrencies. This version of the guidelines assumes that the bank at which the account is held does not directly receive any cryptocurrencies.

The token issuer has the cryptocurrencies converted into fiat money through an exchange regulated by Swiss law or equivalent laws or by a third-party bank regulated by Swiss law or equivalent laws and then transfers the corresponding funds to the bank at which the account is held.

These guidelines recommend requiring the token issuer, regardless of whether or not it is subject to the AMLA, to apply the KYC, AML and sanction standards applicable in Switzerland to the receipt of funds when accepting cryptocurrencies.

Furthermore, the receipt of payment tokens within the scope of a token issue may essentially be treated as a cash transaction. However, it should be noted that every transaction is stored in the blockchain and there is a risk of violating sanctions with transactions in cryptocurrencies, regardless of their amount. The form of token and applicability of the AMLA also give rise to additional obligations.

Institution-specific instructions may create additional requirements or set threshold values that deviate from the guidelines. Internal instructions always take precedence over the guidelines.

Measure / check	Recommendation
4.1 Accepted cryptocurrencies	In principle, the cryptocurrency should be suited to a wallet analysis. Deviations must be justified.
4.2 Issuers of tokens (general)	Information about every subscriber, which should be collected by the token issuer, is generally derived from the requirements of the applicable rules (e.g. CDB, AMLO-FINMA, SRO rules and the FINMA circular on video and online identification). On this basis, the issuer should obtain the following information: name, address (including country), date of birth, nationality and place of birth. The information gathered should also contain relevant wallet addresses (public keys) from which the investors send the capital contribution. Regardless of whether or not the issuer is subject to the AMLA, it is expected that the identity should be established and the beneficial owner determined pursuant to the AMLA/AMLO-FINMA/CDB, at least where the subscription amount exceeds CHF 15,000. Any further measures to increase transparency serve to mitigate risk, in particular in view of potential violations of sanctions. The information collected in the identification process should also contain all relevant wallet addresses that the investor uses when making capital contributions. It is generally appropriate to document identification and beneficial ownership in line with the existing processes of the respective institution. If the bank intends to require documentation about the investors from the issuer, this must be stipulated in the contract between the bank and the token issuer. The bank must take appropriate steps to protect the personal data of the investors (subscribers/participants/token recipients). Beneficial ownership should be documented in accordance with the existing processes of the institution concerned. Identification of the beneficial owner of the assets can be confirmed by means of a requirement for a transaction to be digitally signed or for a microtransaction to be sent using the issuer's public key. The issuer can arrange for the procedure or microtransaction to be certified in a public deed.
4.3 Issuers of payment tokens (specific)	Issuers of payment tokens are subject to the AMLA. They must therefore comply with procedures for the receipt of assets from investors in accordance with the requirements of anti-money laundering legislation as set out in detail in, inter alia, the AMLA, FINMA Circular 16/07 "Video and online identification", and the regulations of the self-regulatory organisations. For issuers of payment tokens, the simplified due diligence obligations set out in Art. 12 para. 2 let. d AMLO-FINMA apply to transactions below CHF 3,000; copies of investors' identification documents need not be authenticated.

4.4	Check of risk databases	The issuer should compare the subscribers against risk databases customary for the industry (in particular politically exposed persons [PEP] and terrorism and sanction lists). On request, details of the comparison should be provided to the bank together with the internal guidelines on the monitoring of PEPs and sanctioned clients.
4.5	Background check (source of funds) and risk assessment of the wallet addresses used by the investors (AML)	It is generally recommended that issuer take a risk-based approach to the background check. A general tracing of the source of the funds in the blockchain has so far not been required. In principle, all additional transparency that the issuer provides serves to mitigate risk. In special cases or instances of specific suspicion in particular, it is recommended to carry out a thorough check by means of a wallet analysis or additional documentation (e.g. additional due diligence instead of a simple database comparison in the case of high investment amounts or domicile in a risk country). A thorough check by the issuer is always recommended for subscriptions that exceed CHF 100,000 (individually or cumulatively). This thorough check includes documented comparison of wallet addresses and ICO subscribers. The bank at which the account is held should reserve the right to request information about the investors prior to the receipt of funds and, should it have its own specific suspicions, to request the issuer to carry out further clarifications (e.g. receipt of specific wallet analyses).
4.6	Quality certification of the KYC/AML check	Regardless of whether the AMLA applies, it is recommended that KYC/AML checks be carried out in accordance with the applicable standards. An issuer that is not subject to the AMLA should either employ a financial intermediary or a company specialised in AMLA compliance for this purpose. On request, the results should be disclosed to the bank at which the account is held. The results should also document compliance with internal company PEP guidelines.
4.7	Exchange for conversion from cryptocurrency into fiat money	Crypto exchanges and the conversion of cryptocurrencies into fiat money pose a particular risk for banks as this is where the risks associated with AMLA issues are concentrated. Banks must therefore set risk-mitigating requirements for an exchange: e.g. an exchange regulated by Swiss law or equivalent laws or a third-party bank regulated by Swiss law or equivalent laws. The definition of "equivalent law" should be based on the internal guidelines of the respective bank.

4.8 Suspicion of money laundering	The investor should not be authorised for the issue (unless legally required due to the ban on tipping-off following a report to the Money Laundering Reporting Office [MLRO], Art. 9a AMLA). The token issuer is responsible for excluding the investor. The bank at which the account is held may waive bank client confidentiality for necessary clarifications within the scope of KYC and due diligence of a token issuer on the basis of the corresponding consent of the corporate client in the contract or by means of a separate waiver. The bank should explicitly notify corporate clients of this circumstance and, accordingly, the issuer is recommended to state this transparently in the terms & conditions.
4.9 Sanctions	The issuer is responsible for complying with sanction provisions (e.g. embargo legislation).

5. Due diligence obligations for financing with fiat currencies

When financing with fiat money, the thresholds and duties set out in section 4 regarding identification and determining the beneficial owners in accordance with the AMLA/AMLO-FINMA/CDB apply.

6. Specific business models

In its report of 14 December 2018 entitled "Legal framework for distributed ledger technology and blockchain in Switzerland", the Federal Council notes that the following DLT activities (in addition to the issuing of tokens as discussed in section 3 and section 4) are subject to the AMLA if they are carried out on a professional basis (Art. 2 AMLA):

- Wallet providers that hold clients' private keys in custody and enable clients to send and receive cryptocurrencies have a power of disposal over third-party assets. They therefore qualify as financial intermediaries and, as such, are subject to the provisions of the AMLA. There are currently no rules governing non-custodian wallet providers, which have no scope to intervene in the transfer of tokens.

- Trading platform operators that have access to clients' private keys and thus also a power of disposal over third-party assets, as well as those that work on the basis of smart contracts and can thus exercise a power of disposal over third-party assets by confirming, approving or blocking orders, act as intermediaries between clients in a trilateral relationship. The provisions of the AMLA therefore apply to such centralised trading platforms. Trading platforms that do not exhibit the above characteristics and have fully decentralised structures, i.e. with no scope for the platform developer to exert an influence, are not subject to the provisions of the AMLA.

Assessing the risks associated with corporate clients that provide services in connection with cryptocurrencies or tokens via exchanges or centralised trading platforms can be made easier by taking some of the following aspects into consideration:

Measure / check	Recommendation
6.1 Exchange to convert crypto to fiat	Via an exchange regulated by Swiss law or equivalent laws or via a third-party bank regulated by Swiss law or equivalent laws. The definition of "equivalent law" should be based on the bank's internal guidelines.
6.2 Compliance with AML/sanctions	AML/sanction programme that complies with the Swiss regulations on onboarding and ongoing transaction monitoring
6.3 AML programme	Dedicated and qualified compliance contact
6.4 Trading portfolios	On request from the bank at which the account is held, the trading platform should demonstrate that the assets being traded comply with the registration requirements of the countries concerned (e.g. US securities).
6.5 Supervision	The service provider is subject to the current version of the AML regulations.
6.6 Authorisation	Depending on the existing licence models (e.g. fintech licence)
6.7 Client segment	On request, the DLT trading system should supply further information on the client structure, for example a generic breakdown/geographical origins.

- Exchanges: The purchase and sale of cryptocurrencies or tokens in exchange for fiat or other crypto investments on a professional basis is a bilateral exchange activity that is subject to the AML regulations.

- Under the rules on combating money laundering, cryptofunds understood as collective investment schemes that invest their assets mainly or exclusively in cryptoassets are treated in the same way as other collective investment schemes.

Companies that offer the option of obtaining their services or products in exchange for cryptocurrencies are advised to conduct the background checks discussed in section 4.5 and to apply the threshold values recommended in section 4.2.

Appendix – Glossary

Token

Simply put, tokens are digital, cryptographically secured information units that are stored in a register based on DLT. FINMA classifies tokens based on their economic function and differentiates between payment, asset and utility tokens. Also see the FINMA guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs) dated 16 February 2018.

Definitions of ICO, ITO, TGE, STO and IEO

There is still no general consensus regarding the definition of the terms "initial coin offering" (ICO), "initial token offering" (ITO), "token-generating event" (TGE), "security token offering" (STO) and "initial exchange offering" (IEO). The focus is on issuing unique, transferable information and/or functional units in digital form (coins or tokens) that can represent a wide range of rights, including fungible rights such as debt claims or membership rights in respect of a company, rights pertaining to tangible assets or other absolute or relative rights.

A token may only serve as a means of payment (coin or payment token). It may not confer any contractual rights on the holder. The term "security token offering" (STO) is currently used where tokens expressly embody rights in respect of the issuer. Where an organisation issues tokens for the first time to raise capital for its own financing, the term "initial coin offering" (ICO) or the technically more correct "initial token offering" (ITO) is often used. Depending on their specific design, all tokens may qualify as DLT-based uncertificated rights and/or as securities under financial market law.

The term "initial exchange offering" (IEO) refers to a means of raising capital that is handled exclusively via an exchange, with the exchange taking responsibility for accepting funds and issuing tokens on behalf of the issuer.

In these guidelines, the term "token-generating event" (TGE) means the same as "issuing of tokens", and the two are used interchangeably.

Chain analysis

A chain analysis is intended to provide information about the source of crypto-based assets. Many criteria can be used in the process, e.g. outgoing or incoming payments in certain wallets, connections to the dark net, "mixers" and "tumblers", scamming and/or gambling websites and transactions from or in high-risk countries. The analysis may also include a risk classification of the trading centres from which the wallets in question were supplied.

Distributed ledger technology (DLT) / blockchain

Distributed ledger technology (DLT) is a shared and secure means of managing data on a distributed computer network. In simple terms, a distributed ledger is a database that is spread across a large number of networked computers and, in principle, independently and continuously synchronises and validates data/transactions entered by participants. Participants have access at all times to a verifiable history, which cannot be manipulated, of all information stored in a specific data set. DLT is more broadly defined than blockchain, covering further possibilities.

Blockchain (DLT application)

A blockchain is one possible form of distributed ledger technology (DLT). It is a digital ledger or database that can be continually added to and cannot be altered. A network of computers (referred to as "nodes") executes the software protocol. In principle, the network independently and continuously groups transactions or other data into blocks, validates them and adds them to an existing chain of validated blocks. Blockchains are used, for example, for transactions in Bitcoin, Ethereum and other cryptocurrencies. A blockchain uses a cryptographic signature known as a "hash" to chain blocks together. The hash employs an asymmetric encryption procedure in which every user has a public key and a private key. These are kept in a wallet, which may be stored online, on a computer, smartphone or hardware wallet or even on paper. A public blockchain is distributed, accessible to anyone and operated by a large number of anonymous participants with no intermediary (e.g. Bitcoin and Ethereum). A private blockchain, on the other hand, is operated by one or more network administrators and is only accessible to identified and authorised participants. Hybrid forms also exist, and consortium blockchains, in which the protocol may be public, but only certain participants can validate transactions.

Exchange
Cryptocurrencies can be converted into traditional fiat money such as CHF or into other cryptocurrencies on exchanges.

Crypto / digital assets
Cryptoassets are cryptographically protected digital assets stored in a DLT application (crypto-based assets), the content of which is uniquely documented (e.g. cryptocurrencies and digital rights). A token represents the information recorded in the ledger, over which the holder has power of disposal with the aid of an access code. As a means of payment, a cryptocurrency only exists in digital form, unlike conventional fiat money issued by a central bank such as US dollars or Swiss francs. The most widely known cryptocurrencies at present are Bitcoin and Ethereum, each of which has its own payment system. Depending on its design, a token may be linked to other assets (e.g. a currency, commodity or security), representing these in the form of a digital asset (e.g. an asset-backed token).

Smart contracts
Smart contracts are self-executing computer protocols based on a blockchain that replicate predefined contractual conditions in the form of program code. A transaction conducted using a smart contract is executed automatically if all parties involved meet the predefined conditions. Smart contracts can technically replicate, verify or help to process the content of legal contracts. The computer protocol automatically monitors the predefined conditions and independently carries out the actions agreed by the parties when a specific trigger event occurs. Depending on their design, smart contracts may also constitute legal contracts in their own right.

•SwissBanking

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
P.O. Box 4182
CH-4002 Basel

office@sba.ch
www.swissbanking.org