

**REPORT AND APPLICATION  
OF THE GOVERNMENT  
TO THE  
PARLIAMENT OF THE PRINCIPALITY OF LIECHTENSTEIN  
CONCERNING  
THE CREATION OF A LAW ON TOKENS AND TT SERVICE PROVIDERS  
(TOKENS AND TT SERVICE PROVIDER ACT; TVTG) AND THE  
AMENDMENT OF OTHER LAWS**

<i>Procedure in parliament</i>	
	<i>Date</i>
1. Reading	
2. Reading	
Final vote	

**No. 54/2019**



## **TABLE OF CONTENTS**

	Page
Summary .....	5
Responsible ministry .....	7
Affected entities.....	7
<b>I. GOVERNMENT REPORT .....</b>	<b>8</b>
1. Background .....	8
2. Grounds for the draft.....	11
2.1 Distinctions between terms and overview of current applications...	11
2.2 Main features of blockchain technology.....	15
2.2.1 Structure and functionality of blockchain systems.....	17
2.2.2 Possible applications of blockchain systems .....	22
2.2.3 Concept of the “token economy” .....	25
2.3 Need for regulation .....	36
2.3.1 Overview of the token economy .....	36
2.3.2 Classification of tokens and bases under civil law .....	38
2.3.3 Reduction of currently known risks .....	39
2.3.4 Regulation and legal certainty for the token economy outside of financial market legislation.....	41
2.3.5 Efficient transactions and legal certainty as the basis for the token economy .....	44
2.3.6 Discussion in other countries.....	47
2.4 Government objectives .....	49
2.5 The term “transaction systems on the basis of trustworthy technologies” and the title of the Law.....	52
3. Main aspects of the draft .....	54
3.1 Explanation of the basic token model.....	54
3.2 Activities on the TT system .....	66
3.2.1 Transformation into the TT system.....	66
3.2.2 Types of delegation.....	70
3.2.3 Token issuance.....	73
3.2.4 Other service providers.....	76
3.3 Regulatory approach .....	78
3.4 Due diligence obligations .....	86

3.5	Book-entry securities .....	101
3.6	Scope of the Law .....	113
<b>II.</b>	<b>GOVERNMENT BILL .....</b>	<b>116</b>
1.1	Law on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG) .....	116
1.2	Amendment of the Due Diligence Act (SPG) .....	155
1.3	Amendment of the Financial Market Supervision Act (FMAG) .....	161
1.4	Amendment of Persons and Companies Act .....	169
1.5	Amendment of the Business Act (GewG) .....	171

## **SUMMARY**

*“Blockchain technology” was initially developed for Bitcoin, a private digital monetary system. Blockchain technology functions as a ledger that can securely record transactions. The technology can be used for much more than Bitcoin however. Blockchain technology has been developed by a number of people and organisations around the world and expanded to other application areas.*

*Blockchain technology is important because of its ability to record “information” digitally, practically preventing this information from being copied or manipulated and ensuring that it can be transferred securely between different people. Security is exclusively ensured through mathematical procedures (e.g. encryption technology, cryptography) and defined rules. Blockchain infrastructure is typically provided online and is available to a broad range of private individuals and companies.*

*The applications of blockchain technology are therefore not only restricted to simple transactions of coins or tokens with an exchangeable value between private individuals. Rather, they provide the option for a large range of economic services as assets or rights can also be recorded in blockchain systems in general. This is noteworthy because it means the creation of digital recording of means of payment or assets and the possibility of conducting transactions with no direct intermediary responsible. Thus, companies offering financial services on blockchain systems use generally available digital infrastructure to provide their services. There are already a number of companies that offer services on the various blockchain systems available today, such as digital wallets, custodial services for crypto-currencies and exchanges for virtual currencies. Blockchain technology is also used today to finance companies or projects (e.g. via “Initial Coin Offerings” (ICOs) or “Security Token Offerings” (STOs)). However, it is likely that it will be possible in future to record a much broader range of assets and other rights on blockchain systems and that a number of services related to these rights will be offered. In particular, the low costs for digital transactions will, according to experts, open up new opportunities in fields such as financial services, logistics, mobility, energy, industry, media, and many more. These applications are grouped together under what is called the “token economy”.*

*Because of the rapid pace of development of blockchain technology and its areas of application, it is very important to draft a law abstractly enough to ensure that it remains applicable for subsequent technology generations. That is why the term “transaction systems based on trustworthy technologies (TT systems)” is used for blockchain systems in this Law.*

*The option of recorded assets or, more generally, rights in tokens, raises essential legal questions which must be clarified for the general legal certainty for users of TT systems and TT service providers. An example of this is the legal effect of transferring tokens with regard to the represented right. This legislative proposal on tokens and TT service providers (TVTG) introduces a new legal object so as to enable the recording of the “real” world on TT systems in a legally secure manner and thus tap the full potential of the token economy.*

*The increasing propagation of blockchain applications has already resulted in problematic areas, such as open questions related to customer and asset protection as well as the misuse of this technology for money laundering or other criminal purposes. Such issues should be addressed by means of clear regulations. As blockchain technology is also actively used in Liechtenstein, the government wishes to clarify which requirements will apply for important activities on TT systems (TT services) with this Law. To do so, not only legal certainty is created but customer protection is also improved and unanswered questions in the application of the applicable laws, in particular in the area of due diligence obligations, have been clarified in order to ensure compliance with international standards and extensive and effective fighting of money laundering.*

*The Law on Tokens and TT Service Providers defines a legal framework for all applications of the token economy in order to ensure legal certainty for many current and future business models. In particular, this involves the essential aspects of a token economy such as generating and storing tokens, and not on the regulation of activities relating to the financial market, such as a stock exchange for payment tokens.*

*For securities to be represented in a token on a TT system, and transferred there, via a physical document without any detours, the legal concept of the book-entry system (Wertrecht) has been accepted in Liechtenstein law, and at the same time*

*the interfaces between the securities law and TVTG has been created. Book-entry securities are dematerialised securities where the functions of a certificate can be replaced by entry into the book-entry register.*

*Because of the enormous potential of the “token economy” for large parts of the economy, the government hopes this Law will increase legal certainty for users and service providers to support the positive development of the token economy in Liechtenstein. It therefore does not only face risks that may exist today, but also meets the needs of market participants for more legal certainty in connection with TT systems.*

**RESPONSIBLE MINISTRY**

Ministry for General Government Affairs and Finance

**AFFECTED ENTITIES**

Liechtenstein Financial Market Authority

Regional court

Public prosecutor's office

Office of Justice

Office of Economy

Vaduz, 07 May 2019

LNR 2019-510

P

Dear President of the Parliament,  
Ladies and gentlemen,

The government submits the following report and application regarding the creation of a Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TVTG) and the amendment of other laws to the High Parliament.

## **I. GOVERNMENT REPORT**

### **1. BACKGROUND**

Information technology developments have always had a substantial impact on the financial sector. As computing power has grown, so too have the number of financial services applications. It has also allowed the financial sector to continuously boost efficiency and performance.

In addition to the exponential growth of computing power, computer technology has also enabled several other basic innovations that have had a strong influence on private life and business. These basic innovations include the invention of the Internet and the smartphone, which make it possible to access and share information no matter where we are. In addition, there are offers such as the low-cost and scalable availability of high-performance computers and data storage as



well as enormous progress in the area of artificial intelligence (AI), which in particular goes hand in hand with the advances in computing power.

These developments, which are usually grouped together under the term the “digital revolution” or “digitalisation”, have made fundamentally new business models possible. In the financial sector, companies in this area are called “financial technology” companies or “FinTechs” for short. Since the 1990s, FinTechs have changed or supported an ever increasing number of processes in the financial sector. While the initial focus was on payment services (e.g. PayPal), later there was a shift towards lending to individuals and small companies and financing for start-ups and companies (crowd lending, crowd investing). However, these types of FinTechs mostly use the traditional financial market infrastructure (bank accounts, payment infrastructure, etc.).

Blockchain technology, which was developed in 2008 as a basis for “Bitcoin”, a kind of electronic monetary system, enables Fintech applications which exist without traditional financial market infrastructure.

Bitcoin was initially used as a cash and payment system in particular. Over time, Bitcoin also developed into an investment product for specialised investors, driven inter alia by a strong increase in value between 2016 and 2018. In parallel, more and more “virtual currencies” came into existence, sometimes with very different functions. As the owner of the asset does not need to be disclosed, Bitcoin has also increasingly been criticised that it is used for criminal purposes (e.g. for ransom demands). The first generation of blockchain, which was developed for Bitcoin, has several other problems that make its use for the broader economy difficult, e.g. the enormous amount of energy it requires and the relatively low transaction capacity. Some of these problems have already been solved by more recent generations of blockchain systems. In view of the level of innovation involved in the development of blockchain around the world, it can

be assumed that future generations of blockchain will solve the other outstanding problems as well.

The development of FinTechs has accelerated sharply in Liechtenstein in recent years as well. While almost no applications for authorisation were submitted to the FMA by FinTechs in 2014, the number of applications has risen significantly in recent years. The government and the Financial Market Authority created the “regulatory laboratory” in 2015 in order to support innovative companies in matters related to authorisation and supervision. This approach has proven itself in several respects: While traditional financial services providers usually have clarity about the regulated activities they seek to undertake, with FinTechs it is usually not clear how and whether they are regulated, as this often depends on the specific structure of the business model. By engaging in an in-depth dialogue with participants, the FMA gains valuable knowledge and is able to determine where there is room for improvement in the current regulatory environment.

Since 2015, the FMA has been in increasing contact with FinTechs thanks to the regulatory laboratory: in 2017, there were approximately 100 FinTechs; in 2018, there were over 250. Many of these companies have some connection with blockchain technology. While the initial focus here was on applications in payment transactions, the focus has of late shifted towards developing new tokens in various fields of application, e.g. project financing for the development of a new generation of blockchain. This initial issuance of tokens is commonly known as “Initial Token Offerings (ITOs)” or, more commonly, “Initial Coin Offerings (ICOs)” where highly different arrangements can be found that have effects on financial market regulatory classification. The dialogue with market participants revealed very early on that blockchain posed several fundamental questions that had to be clarified in order to ensure legal certainty.

The Ministry for General Government Affairs and Finance has been spending a lot time on the topic of blockchain since 2016 for this reason. Internal and external experts concluded that the significance of blockchain-based transaction systems went well beyond current applications. The technology has the potential to significantly change large parts of the economy and thus the financial sector. At the same time, it must be determined that practical regulation would greatly increase legal certainty for all participants and thus significantly favour the development of this innovation.

## **2. GROUNDINGS FOR THE DRAFT**

### **2.1 Distinctions between terms and overview of current applications**

“Bitcoin” and “blockchain” have traditionally been closely associated with each other, but they are different things. “Bitcoin” is one of the possible applications of “blockchain”.

“Bitcoin” is a private, digital monetary and payment system that enables online payment with the same quality as cash transactions (known as “electronic cash” (eCash)). The concept of Bitcoin includes all traditional functions of money, i.e. as payment, as a way to store value and as an arithmetic unit. The concept of Bitcoin also however includes an economic model that mainly exists without intermediaries and central banks.

“Blockchain” on the other hand is the technological basis for blockchain and allows secure transactions between private individuals, principally through combining several technologies (in particular cryptography and a computer-to-computer network). In a functional sense, blockchain works as a transaction register.

“Money” is the umbrella term for all forms of payment and exchange that are widely recognised, while currencies are defined as legal means of payment that must be accepted in a country by all companies. State currencies are generally issued by a central or national bank which, depending on their national mandate, are responsible for price stability. Central banks issue physical cash (bank notes, coins) and commercial banks borrow money from the central banks, which they then in turn loan to the economy. The money used by commercial banks is known as book money. Book money represents a claim to cash that can be used in banking through transfers from giro accounts to giro accounts by means of book entries.

However, as Bitcoin was designed as a payment method, but in contrast to a currency such as the Swiss Franc is not issued by a state and in most cases is not recognised as legal tender, Bitcoin is therefore categorised as private money. In the case of currencies, residents of a country are also subject to an obligation of acceptance, i.e. that every debtor may be able to settle his or her debts in the national recognised currency, which is not the case for Bitcoin.

Various terms of classification are used for Bitcoin depending on one’s perspective and intention: Virtual currency, crypto-currency and crypto-money. The terms “virtual” or “crypto” describe a technological form and, for reasons of technological neutrality, are not appropriate to be used as an umbrella term in the context of this Law. As will be explained in more detail below, the Law on Tokens and TT Service Providers introduces tokens as a new legal object to describe all applications. For this reason, this Law also relates to the term “payment tokens” when classifying digital payment methods, which is used as the umbrella term for all payment functions recorded on TT systems. This also includes all legal currencies that have been issued on TT systems.

In order to be able to ensure its value-retaining function, money requires certain stability and intrinsic value. In certain periods of time, currencies achieved this by being backed by gold. Since the 1970s, most important currencies have stopped being fully backed by gold for several reasons. Currencies without any real value backing are known as fiat currencies. Monetary value stability is ensured by central bank policy, such as governing the quantity of money and interest-rate policies. As Bitcoin also does not depend on any other real value (such as gold), Bitcoin in principle also works as fiat money. In the case of Bitcoin, monetary value stability is to be achieved by limiting the amount of money, mathematical procedures and transparent rules on money creation. This feature of Bitcoin has led to intense discussions as, in principles, it is a counter-model to state monetary policy with a central bank.

Discussions about electronic cash as a contrast to book money began with the development of the internet in the 1990s. Whilst some protagonists sought solutions for private reasons (e.g. cypher punks), others demanded new solutions for economic considerations, such as the Nobel prize winner Milton Friedmann in 1999 in an interview<sup>1</sup> with the US National Tax Payers Union (“The one thing that’s missing, but that will soon be developed, is a reliable e-cash, a method whereby in the Internet you can transfer funds from A to B, without A knowing B or B knowing A. That kind of thing will develop on the Internet and that will make it even easier for people to use the Internet”).

As a result of restricting the quantity of Bitcoin in association with a certain amount of energy expenditure to create new Bitcoins, Bitcoin becomes similar to gold, whose intrinsic value is also defined by its limited availability, the time needed to collect it through mining companies and long durability. Bitcoin’s po-

---

<sup>1</sup> See <https://www.youtube.com/watch?v=mlwxdyLnMXM> (viewed on 15/03/2019)

tential to retain value and for investment was recognised by investors early on. The strong price development in 2016 to 2018 in particular led to direct speculation in Bitcoin growing sharply. A short period of time later, financial products such as structured products or investment funds with reference to Bitcoins came into being in order to make investment easier for investors. As with gold, the price of Bitcoin is subject to heavy fluctuations driven by supply and demand fluctuations. The value of Bitcoin has decreased significantly since the start of 2018. In the meantime, its value has restabilised, or even increased, which the Bitcoin community views as proof of this intrinsic value.

In recent years, additional tokens in a wide range of forms have come into being alongside Bitcoin. Although many are initially thought of as means of payment, the idea of using these tokens as an investment is spreading, which is why we frequently speak of “crypto-assets”. This broad use of tokens as an investment has led to intense discussion with authorities and regulators in all states as to whether and how financial market laws are to be applied.

In addition to payment tokens, blockchain technology is also used to issue claims or membership rights to finance companies, but also to issue “utility coins”, coins or tokens with additional functions such as a digital “right of use” to a new blockchain system. The public issue of new tokens or “utility coins” frequently takes place via “Initial Coin Offerings (ICOs)”. In the case of securities however, we speak of “Security Token Offerings (STOs)”. The term “Initial Token Offerings (ITOs)” is mostly used as an umbrella term.

As there are currently various types of coins or tokens, and they are used for different purposes, the following figure provides an overview of the important areas of application today. This should facilitate the classification of discussions.

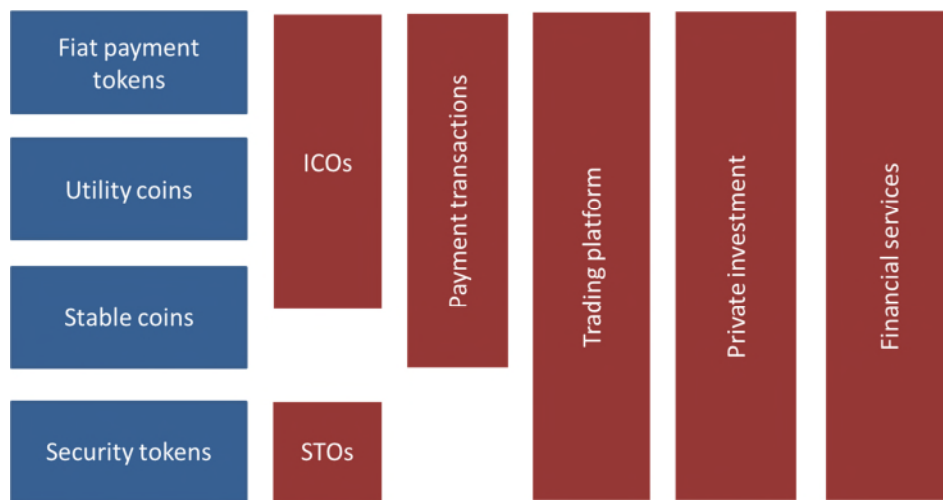


Figure 1: Overview of the current applications of blockchain

## 2.2 Main features of blockchain technology

As blockchain technology in principle was developed as electronic cash, the main features of this technology can be derived via this application example:

a physical bank note provides the advantage in day-to-day life that Person A can directly transfer a monetary amount to Person B. The transfer can be fully completed, i.e. the seller immediately receives the money and without the risk that the money will be taken back at a later date. The complex security precautions with regard to bank notes and coins significantly reduce the risk of counterfeiting.

In the case of electronic payments, such as via a credit card, it is far more complex to achieve the same level of security, which sometimes is expressed in fees. Amongst other factors, the reasons for this lie in a not insignificant risk of misuse (e.g. as the customer sends their full payment initiation data to the seller) and a relatively complex payment and verification process including several service providers and intermediaries.

The need for electronic payment with the quality of physical cash can therefore clearly be seen with the advent of the internet and electronic trade (e-commerce) at the latest and must be viewed, as a result, as a natural development within the context of the digitalisation of the economy. From this perspective, it is fully conceivable and also, in principle, evident, that state currencies such as the Swiss Franc and Euro will issue digital money with the quality of cash in future in order to increase the legal certainty of digital transactions.

If one wishes to reproduce a physical bank note digitally, a significant problem arises: Even if the “realness” of a digital bank note can be ensured via technical procedures, a digital bank note may be copied with no loss. The consequence would be an uncontrolled, growing quantity of money and a loss of trust in the circulation of money. Implementing digital cash (in contrast to digital payment with book money which is processed via banks) has for this reason not been possible with the requisite security for a long time from a technical perspective. Blockchain technology has solved this problem and therefore paved the way for digital cash.

In contrast to the traditional digital payment process, no intermediaries assuming security and quality are required for blockchain-based transactions. The guarantee function is assumed by unchanging rules represented in the technology. The strong security of blockchain technology is derived from the combination of various features, such as the use of encryption technology (cryptography) and the distribution of the transaction register (main ledger) to a high number of computers connected via the internet (computer-to-computer network, peer-to-peer). For this reason, we frequently speak of “Distributed Ledger Technologies (DLTs)”, i.e. the technology of the distributed or decentralised main ledger. Blockchain technology is developing rapidly. Even today we can see blockchain



generations which are neither based on asymmetrical cryptography nor on a decentralised main ledger.

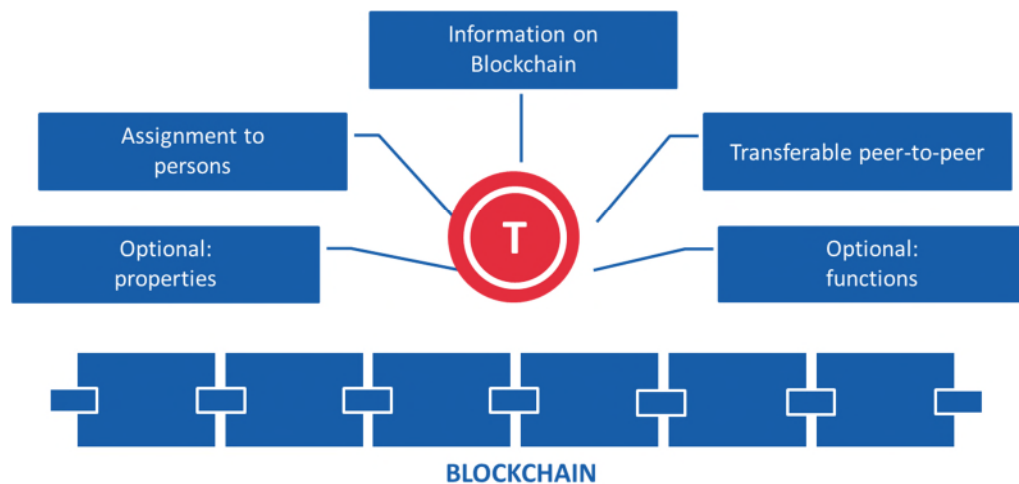
Blockchain technology therefore enables the holding of rights to a digital object and the clear and secure transfer of the digital product to another person. In this process, the second person can rely on the fact that the first person may no longer dispose of the object and has also not made any copy. Blockchain therefore creates a sort of “uniqueness” in the digital world which was not previously possible. Digital objects or information can be transferred with greater security, information with regard to falsifications and the same “functionality” such as similar certificates, in principle such as objects. The digital space allows however for quick transactions between two people across the world.

One of the most important innovations of blockchain is the invention of “digital originals” or “digital certificates”. Blockchain ensures that the original is not duplicated, that it is clearly assigned and that it can be transferred securely.

This quality is not only a fundamental requirement for a digital “bank note” but also for all areas of application in which – abstractly formulated – digital information cannot be copied and, at the same time, should be provided for legal communication, such as digital securities.

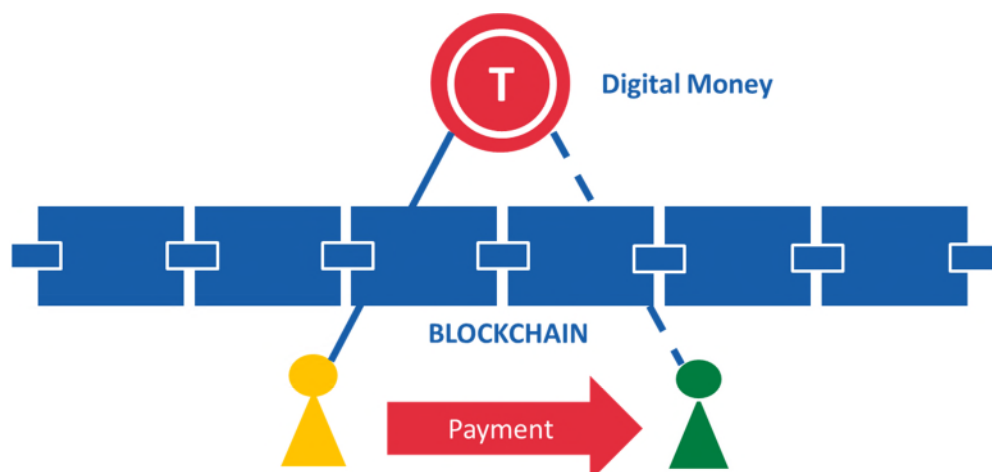
### 2.2.1 Structure and functionality of blockchain systems

The following chart provides an overview of the typical elements of a blockchain system:



**Figure 2: Overview of the typical elements of a blockchain system**

The core of a blockchain system is information, which is clearly attributable to one person and can be securely transferred to another person. Such information may be structured very differently and may also assume different functions. For example, it can represent digital money such as Bitcoin. The key holder can transfer digital money to a third party using blockchain technology. The blockchain, together with user interfaces (e.g. a wallet app on a smartphone), thus functions as a payment system.



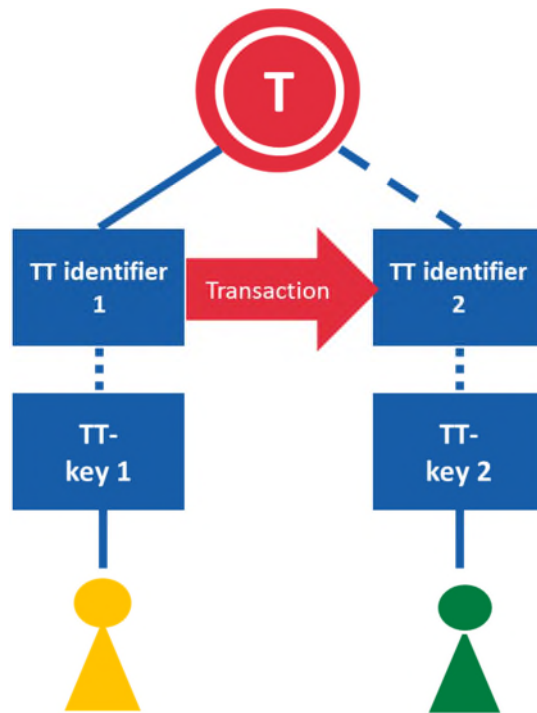
**Figure 3: Illustration of a payment using digital currency on blockchain**

On some systems, this information is called a “token”, in reference to the English term for a private minted coin or “token”. There are some blockchain systems,

such as Bitcoin, in which this information is not named a token, but a coin, yet the term symbolises the independence and portability of this information. For this reason, the Law uses the term “token” for all types of technical implementation.

Blockchain system technology ensures that this information cannot be used twice (“double spending”). It is therefore not technically possible to make copies. As a result, blockchain technology fulfils the ideal conditions for digitalising assets.

On blockchain systems, tokens are clearly allocated to an identifier, and therefore directly to a user (a person) through an entry in the blockchain protocol. Users therefore assume liability for this identifier. Most current blockchain technologies are based on so-called asymmetrical cryptography, in which the address is generated from the “public key”. The address can therefore be publicly disclosed so other persons can transfer tokens to the user. In cryptography, the public key is always associated with a “private key” that makes it possible to approve or sign transactions. As asymmetrical cryptography is only one of the possible solutions for the functionality of blockchain, the technologically neutral term “TT identifier” is used in the Law for “address” or for “public key” and “TT key” is used for “private key”. “TT” stands for “trustworthy technologies” (see section 2.5). In functional terms, every transaction system requires identifiers to which tokens can be assigned and keys with which tokens can be disposed of and a transaction triggered.



**Figure 4: Illustration of how blockchain works – transferring tokens between two identifiers**

In order for a person to transfer tokens to another person, the token shall be assigned to the “identifier” of the other person by signing a transaction with the “key” of the sender. In this way, transactions are stored in immutable form in the blockchain record and visible to all system participants.

With Bitcoin and many other blockchain systems, the transaction record (blockchain) is saved in a decentralised manner by all (full-fledged) participants in the system. Thus, all participants have a copy of the record on their computer. Before a transaction is executed, whether the sender can really dispose of the token will be verified. Only then is the transaction entered in the record and distributed to all participants. Transactions are grouped in blocks and each block is associated in cryptographic terms with the previous block. As a result of this process, the amount of computing power needed to manipulate the blockchain (decryption) is so great that it is safe to assume that these records cannot, in prac-

tice, be manipulated. Technological progress in computing power will likely be offset by improvements to cryptographic methods.

This description is intended to show how blockchain technology can ensure the integrity of tokens, their allocation to an individual and to a transaction without having an intermediary monitoring them.

With blockchain technology, tokens are only assigned to an “address” or identifier in the decentralised transaction record. Thus, this information is, in principle, stored in a publicly accessible system like the Internet. Accordingly, those who have knowledge of the key can – provided he/she has access to the Internet – transfer tokens directly to another person without the need for an intermediary, such as a bank. This is referred to as a “peer-to-peer” transfer, i.e. directly from one person to another person.

In the case of digital money, this means that money can be transferred directly from one individual to another individual. In practice, this can be done, for example, via smartphone: A user can store his/her public key and private key on his/her smartphone using a “wallet app”. To initiate a payment, the sender simply takes a photo of the recipient’s public key or an “address” derived from such in the form of a QR code, enters the amount and approves the payment. Depending on the blockchain system, the money is assigned to the recipient immediately or within a few minutes.



**Figure 5: Address “12c6DSiU4Rq3P4ZxziKxzl5LmMBrzjrJX”  
in a depiction of a QR code**

Additional features and functionalities can now also be programmed in tokens. For example – and this is very important for the token economy – they can now be used to represent real assets or rights (see section 3.1), or the transfer can be restricted on the basis of certain rules. The functions can be based on so-called “smart contracts”, which automatically carry out transfers of tokens in line with the contract.

### 2.2.2 Possible applications of blockchain systems

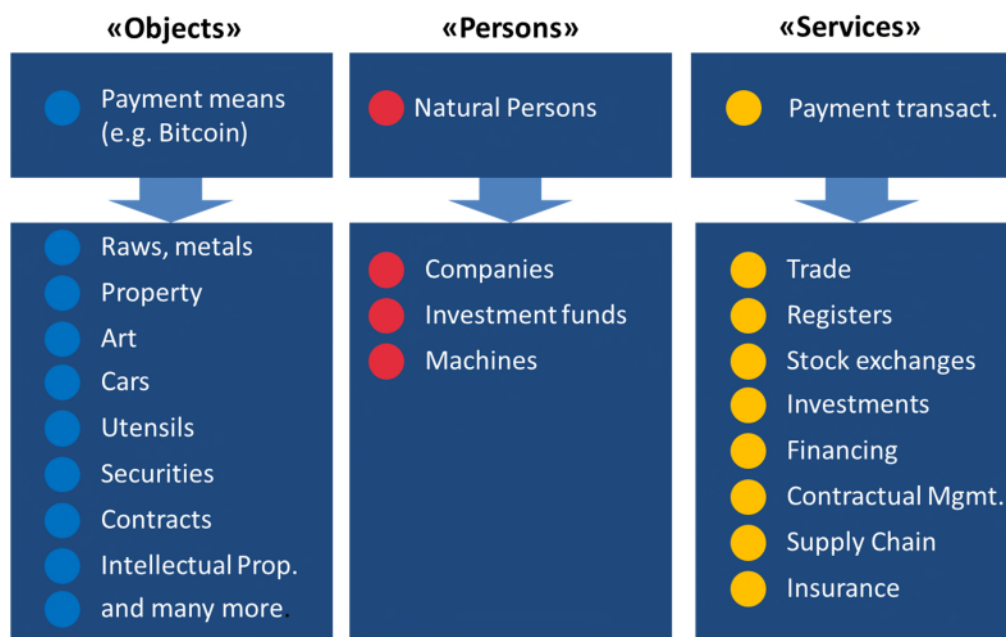
As already described, payment transactions are a possible use of blockchain. Blockchain makes it possible for private individuals to carry digital money with them in a kind of digital wallet and transfer the money to other individuals. The other network participants provide the confidence that the payer is the owner of the money and that the transaction will be carried out securely. It is now possible – by omitting the otherwise necessary intermediary chain from the payment process – to reduce the time required for transfers substantially.

Another related field of application is the trading and administration of securities, such as stocks and bonds. Although this process is already largely digitalised, the costs to list, store, transfer and administer securities is still relatively high. One side effect of this is that only large companies are able to benefit from the opportunities on the financial market.

The use of distributed ledger technologies such as blockchain could reduce the barriers to entry to the financial market substantially and thus offer medium-sized companies the opportunity to obtain simpler and more sufficient financing.

The storage and transfer of digital money as well as the administration of securities will become a more important application area for blockchain technology in future. However, the government anticipates that the areas of application for blockchain will go far beyond these. Firstly, the range of assets traded on block-

chain systems will likely become much larger: From rights to precious metals, precious stones and commodities to rights to works of art, property and real estate and rights to used items such as cars, watches or yachts, in future comprehensive rights to economically relevant goods may be represented in blockchain systems. This enormous scope of applications of blockchain systems is usually grouped together under the term “token economy”.



**Figure 6: Illustration of scope of application of the “token economy”**

Secondly, blockchain technology enables trade and exchange activities to be carried out worldwide in a more efficient and secure way which are mainly carried out today physically or in personal contact. This will first of all have significant effects on direct (private) economic processes. Second of all, we can expect that efficient trading platforms that have only previously been open to selected assets will also be available for smaller and less liquid assets based on blockchain technology. This means that SMEs will have easier access to capital markets. This means that in future new options outside of recognised trading platforms such as regulated markets, multilateral trading facilities (MTF) and organised trading

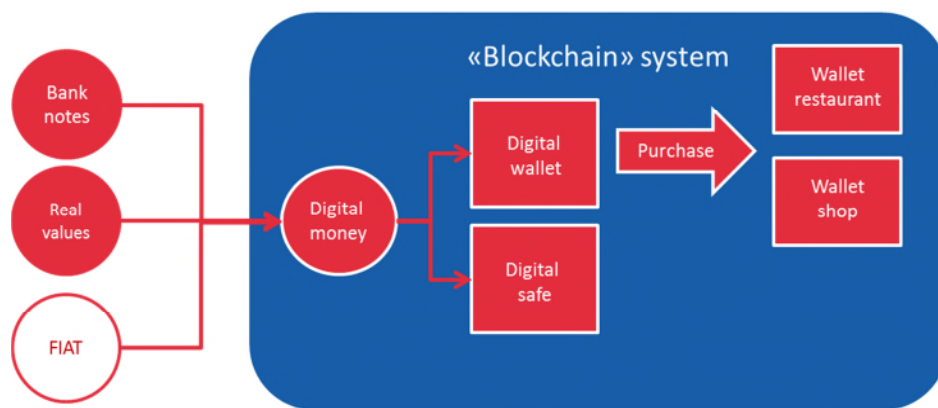
facilities (OTF) will open up, starting with simple exchanges between two individuals and assuming many different features, such as a blackboard function.



### 2.2.3 Concept of the “token economy”

To better illustrate the possible applications of the token economy and for a better understanding of the activities defined in the Law, several use cases are described below:

#### 2.2.3.1 Digital payments



**Figure 7: Illustration of applications of digital money**

The possibilities of using digital payment via tokens are as extensive as the economy itself. Digital money forms the basis for the token economy and can be used in every one of the cases of application described. At this point, only a few examples can be given to illustrate its potential:

#### **Online shopping**

Various procedures are used (credit cards, payment service providers, by invoice, by advance payment, PayPal) for purchases in on online shop that are associated with significant fees for both parties, and sometimes also with time delays.

With digital money (cash), a purchase can directly transfer money without any fees or with low fees and transfer further risks to the seller. The seller is also certain that they will receive the money. It is also conceivable that the transfer of

money to the seller will be coupled with successful delivery (see “smart contracts”).

### **Payment in restaurants**

As part of digitalisation, in future more and more restaurants will receive orders digitally, i.e. via a tablet or smart phone, in order to design internal processes more efficiently. As small transactions are also possible with digital money (cash), digital payment can also be made per dish/drink with the order directly. This means that restaurant visitors experience less waiting time.

### **Payment for the use of car sharing services**

Car sharing is the shared use of a pool of cars for a group of persons. User fees can be automatically and directly paid with digital money. For example, this means that a base fee is transferred to the service provider directly when entering a vehicle or a continuous fee per kilometre drive is paid directly. Such micro transactions, which in future will be common within the context of the Internet of Things, are based on a low-cost, efficient money transaction that is automatically settled.

For digital money to function properly it must have broad acceptance, intrinsic value as well as transparent and liquid trading in order to ensure sufficient price stability.

Digital payment methods can have different foundations:

- a) they may be directly backed by legal currencies, i.e. customers have the right to convert digital payment instruments into the legal currency at any time;
- b) if a central bank issues digital payment instruments on blockchain systems, the digital payment instrument directly assumes the function of cash;

- c) payment tokens backed by a real assets (e.g. gold): the holder of the digital money has the right to draw the underlying asset at any time; and
- d) Fiat – payment tokens (e.g. Bitcoin): Function as a payment instrument is achieved through the system rules and not by a connection with an asset.

Digital money is then managed in a so-called digital wallet and, like bank notes and coins, is available for transactions. These wallets can be installed as an app on smartphones.

#### 2.2.3.2 Company financing

If a company would like to increase its capital today, it can do this either through private investors or the financial markets, e.g. an IPO. The financial markets route is associated with considerable costs and, most of the time, is not worth it for many smaller and medium-sized companies.

The digital representation of a claim or membership right (e.g. a share in a block-chain system) essentially allows for the secure transfer of this right between two persons, and therefore the attractive option for investors to efficiently resell their claims or membership rights on a secondary market (see more below). Naturally, transfer requirements or restrictions, such as in the case of restricted shares, must also be complied with in the digital sphere.

New claims or membership rights can now be issued at various levels:

- 1) Private financing Private selling by the company to investors is just as possibly digitally as without blockchain. With blockchain, new efficient options are now available in particular for generation, managing registers and administration (voting rights and the payment of dividends), which can be complex at present.

For investors, blockchain provides access to more opportunities to resell rights on the secondary market.

2) Own issue: A company may itself publicly issues new claims or membership rights online and receive payment via payment tokens without requiring a bank to do so. Naturally, the company must consider the relevant laws when doing so (e.g. the Securities Prospectus Act [*Wertpapierprospektgesetz* -WPPG]) or the Due Diligence Act (*Sorgfaltspflichtgesetz* - SPG)) in the same way as without blockchain. The advantage for the company is the access to a larger network of investors online associated with a lower base expense per investor, meaning that also smaller denominations can be offered. In turn, this allows for investors with smaller investment portfolios to invest.

3) Service provider issue: If the company uses a service provider for the public issue, this normally falls within the area of financial market regulation (such as the Banking Act) which governs who may issue securities. As a result of securities being able to be sold directly to investors thanks to blockchain technology, the transaction costs are in general lower and gives a broad range of investors access to smaller and medium-sized companies.

#### 2.2.3.3 Trading with securities

Blockchain technology enables secure transactions of securities at various levels:

1) Direct sale between private individuals: In technical terms, just like payment tokens, the securities of a private individual can be saved in wallets and transferred directly to another private individual. This option exists both physically and online. With transfers, the relevant transfer requirements and restrictions must be complied with, such as bearer shares being entered into a register (arti-

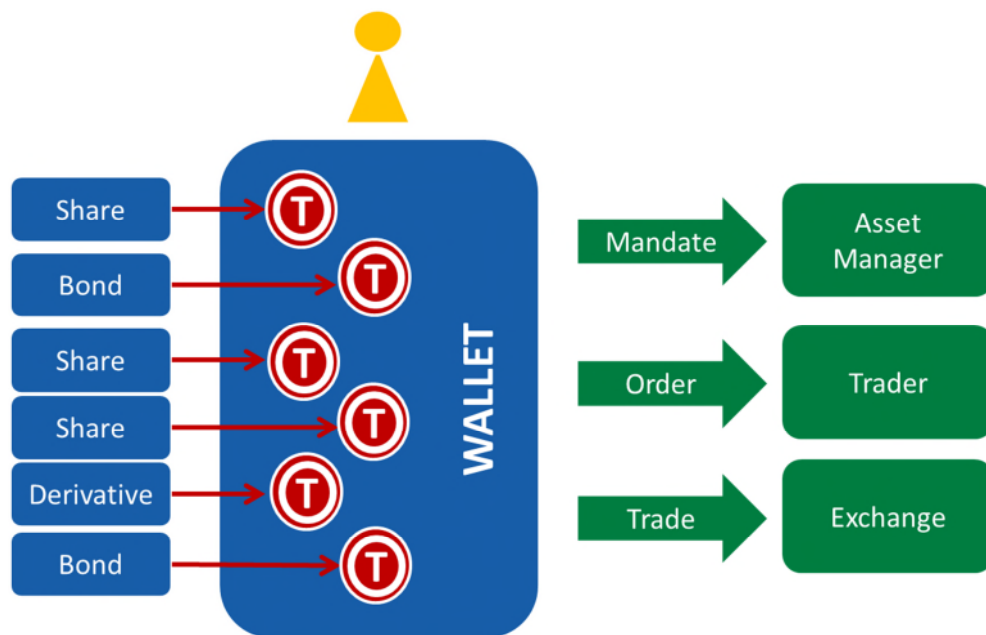
cle 326 PGR [*Personen- und Gesellschaftsrecht* - Liechtenstein Person and Company Law]).

2) Use of an internet platform to find potential purchasers: There are already platforms which bring the purchasers and sellers of securities together, however they do not influence pricing or the execution of a transaction. They primarily work as a kind of “notice board” function.

3) Use of a trading platform: Similarly to the traditional financial market, the functions of professional trading platforms are also offered for tokenised securities. These include bringing a number of purchasers and sellers together, concluding transactions, the inclusion of professional traders and the publication of price information. Operating a multilateral or organised trading system or a regulated market (“stock exchange”) for securities is regulated.

#### 2.2.3.4 Asset management

The assets recorded on blockchain systems can also serve as the basis for the provision of services by professional asset managers. Asset managers can receive a partial right of disposal from their customers over a so-called wallet, a digital portfolio, so that they can make investment decisions on behalf of the customer and, if necessary, issue a mandate to the trader for the purchase/sale.



**Figure 8: Illustration of the possible financial services on blockchain systems**

The conceptual difference between blockchain-based transaction systems and the traditional financial transaction system is the detachment of the assets from the service provider. This not only makes it easier to specialise but also to switch service providers.

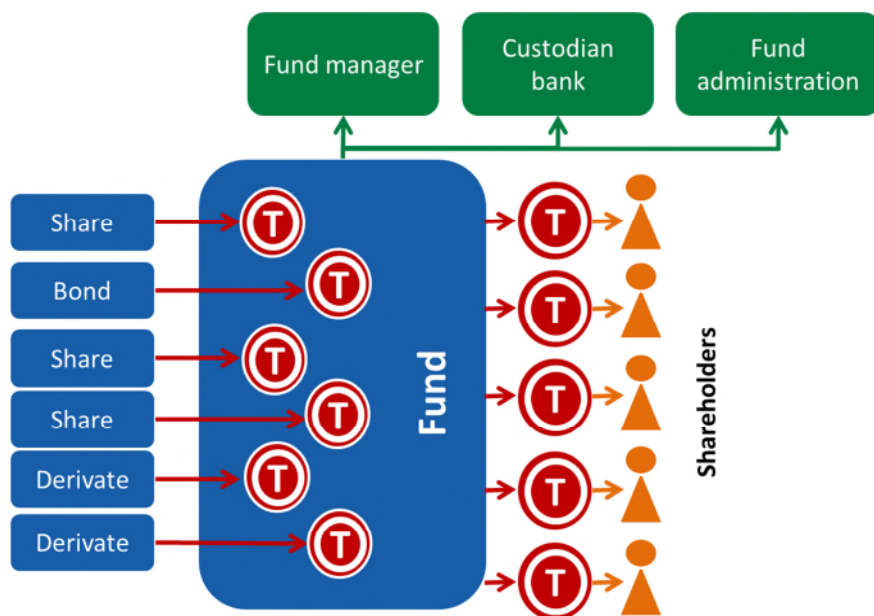
#### 2.2.3.5 Other assets and management

The lower entry threshold for assets in a secure transaction infrastructure results in the ability to use a very broad investment horizon as the basis for services. This, for example, allows an asset manager or one of the service providers described above to provide their services across the customer's entire asset portfolio, and – in the case of special investments – a greater likelihood of finding a specialised service provider (e.g. valuation, pricing).

#### 2.2.3.6 Funds

Investment funds can be set up on blockchain systems as well. The fund's unit rights are recorded in tokens and, as a result, these rights generally can be trad-

ed. The fund scheme according to the AIFMG (Alternative Investment Fund Manager Act), UCITSG (Law on Undertakings for Collective Investment in Transferable Securities) or IUG (Investment Undertakings Act) must be applied when the management of the fund share certificates is recorded via the blockchain system. These applications are also attractive for this year as certain regulatory requirements can be met using technological means ("look through").



**Figure 9: Illustration of a fund structure based on blockchain systems**

#### 2.2.3.7 Luxury goods

Ownership, licensing and warranty rights for luxury goods can be uniquely recorded in digital form and be assigned to a person via an address by using blockchain systems. Companies can directly record these rights digitally when they produce the goods and then transfer them to the purchaser via a blockchain system when the product is purchased. The purchaser can then provide reliable proof of ownership, for example, to the customs authorities. The luxury item can be identified using the serial number or qualified technical procedures. If there

are several copies of a serial number in circulation, the legal owner can be identified using the digital deed of title.

This example also reveals other advantages of the token economy: Because the “warranty rights” are managed in the owner’s “digital wallet”, it is no longer necessary to have a sales receipt or other proof of purchase for the warranty. If necessary, reliable proof of the warranty right can be provided to the merchant or the company that produced the item.

Additional services can be linked to the digital record as well: For example, product-related valuables insurance can be taken out directly at the time of purchase, as proof of the item’s existence, ownership and possibly its purchase price is clearly recorded in digital form. It is also easier to track a theft, as an item that has been reported stolen is easier to identify without digital proof of ownership.

#### 2.2.3.8 Music licensing rights

Digital music (e.g. an MP3 file<sup>2</sup>) is generally easy to copy. This problem can be solved with the concept of the blockchain by recording the “right to use” the music and allocating this right to the legal purchaser in a secure manner. This ensures that the right can only be transferred (if permitted under the terms of purchase), but not copied. This leads to greater legal certainty for artists and production companies. However, this could also result in models with greater legal certainty for consumers as well, as the acquired “licensing right” to the music is assigned directly to them, irrespective of any intermediary, platform or technology.

---

<sup>2</sup> MP3s are a process for the lossy compression of digitally saved audio data.



#### 2.2.3.9 Smart Contracts

Smart contracts are regulations formulated in computer code that are automatically executed by a platform. This may be simple exchange transactions such as the payment of a monetary amount when goods are received. However, significantly more complex options are conceivable, in particular in connection with the Internet of Things in which many everyday items or machines are connected via the internet. Many options for automation in these visions are connected with smart contracts: The automatic payment of a monetary amount when a car is opened by a certain user in a car sharing pool can be implemented via a smart contract. The idea that a fridge directly orders and pays for goods can frequently be found in a smart contract.

#### 2.2.3.10 Blockchain for car files

Blockchain technology can also be used to improve the legal certainty and transparency of car sales by managing a digital car file, which will save all relevant information during a car's life cycle and protect it from falsification. For example, all maintenance activities, sale transactions etc. can be recorded meaning that a purchaser can have an overview of the car's whole 'history' when making a purchase. The risk of fraud and mis-information is therefore considerably reduced.

#### 2.2.3.11 Tracking medication/food

For some medications and foodstuffs it is essential that the product be guaranteed throughout the entire transport cycle and stored within a certain temperature range. By saving measurement data in a blockchain, this proof can be provided at relatively low cost, in a way which protects it from falsification.

In addition, the original certificate can be incorporated in a way which protects it from falsification with blockchain, where fraud and counterfeit products can be recognised more easily, both with regard to foodstuffs and medication.

#### 2.2.3.12 Supply chains

Supply chains in industry or shipping also require different stations to be recorded precisely and in a way which protects from falsification. This is in particular a problem if a number of interim stations are required in international trade (e.g. ships, lorries etc.). These supply chains can be implemented transparently, with greater security and with lower costs with blockchain technology by recording every transaction in the blockchain.

#### 2.2.3.13 Drinks vouchers at festivals

Blockchain technology can also be used for “simple” vouchers, such as drinks vouchers at festivals. The digitalisation of vouchers could simplify certain processes such as buying a voucher (e.g. a direct purchase via an app or a website where queuing is not necessary). This would also be possible, theoretically, without blockchain, but with blockchain a festival operator could access an existing infrastructure with greater legal certainty (wallets and transactions). As a result, users have greater legal certainty by being directly sent the voucher and this voucher being functional and therefore valuable as such, without involving the festival operator themselves.

#### 2.2.3.14 Interfaces with other fields of law

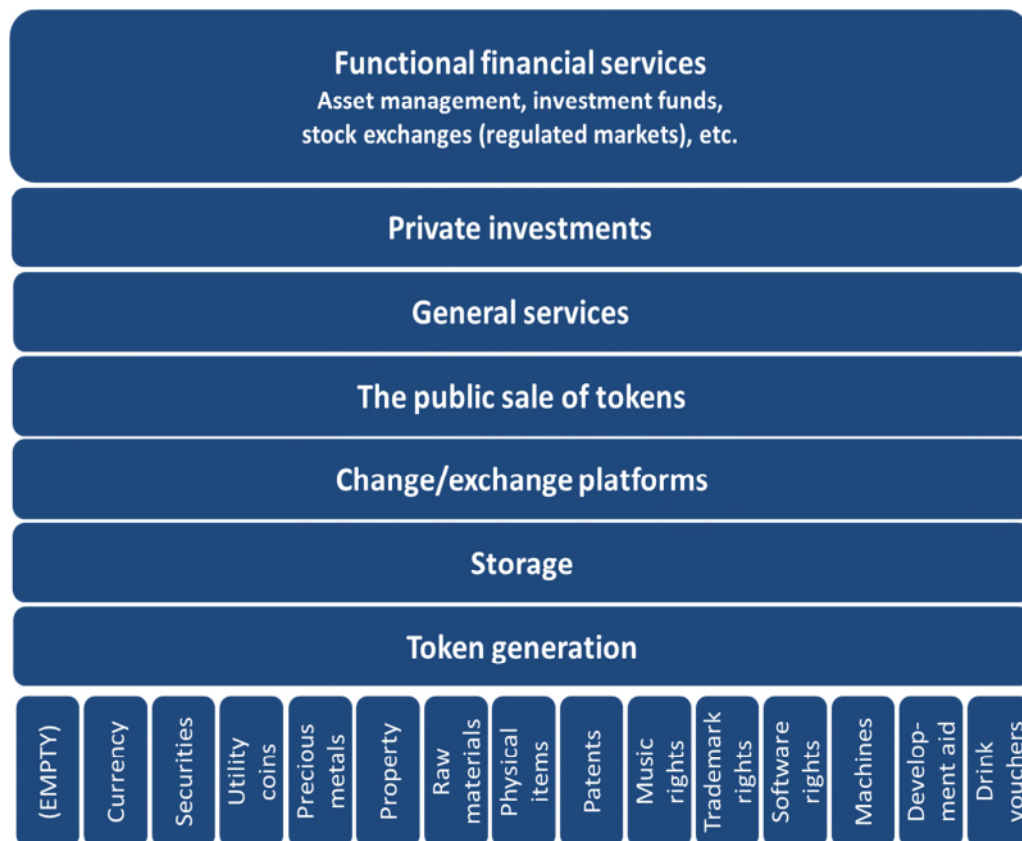
In addition to the TVTG, some potential applications of the token economy are also based on other fields of law (e.g. financial market law, company law, real estate and property law). The TVTG is a framework law which is intended to offer

an appropriate legal basis for token-based applications. In addition, special legal regulations must continue to be observed. On the one hand, this means that the requirements for certain activities may be higher, for example, if they fall under the scope of financial market laws, and on the other hand that even with entry into force of the TVTG not all applications will be immediately possible, and – if politically desirable – they will have to be implemented in separate projects.

## 2.3 Need for regulation

### 2.3.1 Overview of the token economy

Figure 10 illustrates the fundamental value creation chain of a token economy in connection with the larger range of objects that can be digitally recorded in a token economy. It shows that certain functions that are currently seen and discussed in connection with crypto-currencies in particular are also important for all other objects.



**Figure 10: Functional overview of the token economy**

**Token generation:** Tokens must always be generated before they can be used for other activities and functions. When a token is generated, information is introduced to a transaction system and is available a priori to the generator or the client of the generation. Merely introducing a token to a transaction system is

not considered to be a public sale. Most tokens are put into circulation via generation. When tokens are generated, asset objects and rights must be correctly recorded in digital form in order to ensure sufficient legal certainty.

**Storage:** Keys may in general be stored by owners themselves. As assets can also be lost when keys are lost, various forms of professional service providers are established for storage in order to increase comfort and security for owners.

**Exchange and trading platforms:** The base transaction in a token economy is the direct exchange between, for example, private individuals or (commercial) companies. This essentially means daily business transactions (cash in exchange for services or a product) that can be made more legally certain through tokens. In addition, tokens of all kinds are exchanged, i.e. private individuals can resell their tokens (e.g. ownership tokens to a bicycle) to other private individuals. This functionality is then rather similar to private internet exchange platforms such as eBay, tutti.ch, etc.

Crypto-exchanges partly fall under simple exchange platforms in which private individuals exchange payment tokens without the platform itself being able to intervene or be involved in the transaction.

Exchange and trading platforms can always be functionally expanded, for example with pricing mechanisms or mechanisms for assigning orders. This is in particular the case if large volumes of the same tokens are traded.

This is conceivable in general for all token applications, but only practically relevant for certain types of tokens if the required trading volume is reached.

**General services:** As described in chapter 2.2.3, token can be used for many activities and services outwith the financial market.

**Private investment:** All tokens may in principle be used as investments by private individuals. It is important to understand that these private investments do not need to involve financial service providers (these services are included at “financial service” level), but are purely the private holding of assets, such as works of art or unlisted shares.

**Financial services:** The functionality of financial services applies in principle to all areas of application. Investors will also request services such as investment advice or asset management for other tokens, such as “art tokens” or “real estate tokens”. Crypto-exchanges may also have functions and volumes that are highly similar to a regulated market (stock exchange).

It is important to understand that the entire token economy cannot be equated with the financial market, but that financial services only include a small, though important, part. Many fundamental activities must however be provided outwith financial services.

### 2.3.2 Classification of tokens and bases under civil law

A token economy needs a model for tokens. In other words, it needs a model for recording a large range of assets and rights on a digital transaction system and for handling the tokens.

The legal classification of tokens is therefore of great importance. As Bitcoin was the first application of a blockchain, the discussion in many states focuses on “virtual currencies” with regard to payment tokens or on what are known as “utility coins”. From the perspective of the token economy, it will however quickly be clear that too narrow a classification of tokens (e.g. as a crypto-currency or as a crypto-asset) excludes many sensible applications of the token economy. This is why, for the government, it is clear that another approach must be taken that does justice to the potential of the token economy.

The nature of tokens is novel to the legal system. For this reason, it is not possible, to an appropriate extent, to clarify certain fundamental legal questions with regard to tokens based on existing laws.

In addition, when recording assets on a digital transaction system, there are further levels of complexity with regard to the interaction between the digital and “analogue” world, which have not yet been clarified, but that are of great significance for all users of TT systems.

### 2.3.3 Reduction of currently known risks

Because blockchain technology has now been in use for more than ten years, various experiences concerning the risks and challenges presented by this technology have been gained. These risks can be reduced through effective regulation.

Despite the high level of security of the blockchain technology itself, i.e. the function of the transaction register, it is in principle possible for assets to be stolen. The main point of attack in this regard is private keys which are either stored by the person possessing the right of disposal themselves or the service providers in “wallets” (“storage” function in figure 10). In the past, computer hackers were able to create access to “wallets”, thereby transferring millions without authorisation on multiple occasions, mostly as a result of the carelessness of users but also software weaknesses<sup>3</sup>. As a result, software weaknesses have been corrected and the risk of such unauthorised transfers is reduced. However, there is – as with every IT system – a race between hackers and software providers. Using the systems remains, however, a main area of attack.

---

<sup>3</sup> These are not weaknesses in the Bitcoin protocol but in additional software programs provided by third-party providers.

From the perspective of the owners of assets, there are several basic questions, the answers to which are extremely important for the legal certainty and the propagation of these systems. Firstly, the question is raised as to how the legal system needs to handle theft or similar offences. If a private key is illegally copied or the hardware wallet in which the private key is saved is stolen, both the “owner” and the perpetrator may dispose of the token. Proof of “ownership” is no trivial matter in many cases in such an instance. If the perpetrator can be identified, further questions are raised after the token is returned to the injured party. Because the blockchain cannot be manipulated, or can only be manipulated with extreme difficulty, the transaction cannot be simply deleted. If the perpetrator has transferred the token to a third party in good faith, further questions arise about how to resolve this situation. Similar questions arise when the private key is stored by a service provider (e.g. a wallet provider or a crypto-exchange). In such cases, the relationship of the legal owner with the service provider is important.

In this connection, there are also important questions related to the bankruptcy of service providers who store tokens or private keys on behalf of customers. It is not currently clear in all cases whether these tokens are included in bankruptcy assets or can be segregated.

It is an important duty of the state to offer answers to these questions related to ownership, delegation and abuse in order to ensure a high level of legal certainty for all stakeholders.

Another risk is presented by service provider fraud. Embezzlement may affect the entrusted assets (e.g. wallets or crypto-exchanges) by using the assets they contain contrary to agreement. From a consumer protection perspective, the safekeeping of tokens is a central issue and should be subject to qualitative requirements.

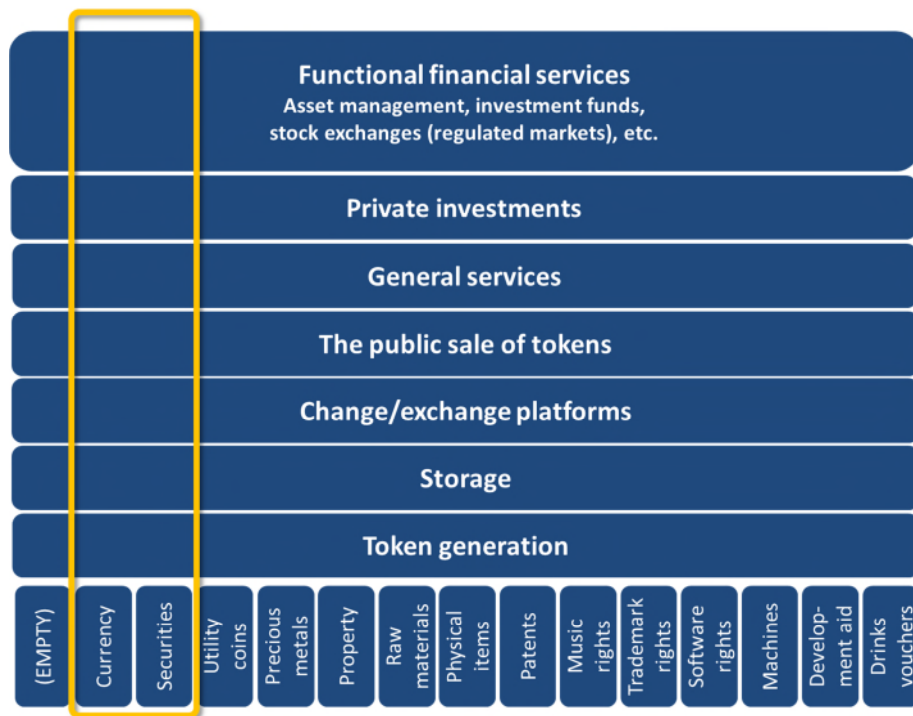


In addition, so-called initial coin offerings (ICO) provide numerous opportunities for fraudulent intentions: There have been an increasing number of cases around the world in which ICOs have been offered under false pretences in order to obtain large amounts of assets.

With current blockchain systems, such as Bitcoin, transactions and the allocation of these transactions to addresses is completely transparent, yet the owners of addresses do not have to be identified. This opens up areas for attack as a result of misuse, money laundering or other illegal transactions that must be effectively combated.

#### 2.3.4 Regulation and legal certainty for the token economy outside of financial market legislation

Financial market regulation is essentially technology-neutral and, for this year, also applies to regulated activities on TT systems. The area of application of the financial market regulation is connected in many cases with terms such as legal currency, securities or financial instruments. It is therefore clear that all tokens representing currencies, securities or financial instruments are also to be classified as such in accordance with financial market regulation. This means however that with regard to tokens that represent other rights and are not to be classified as financial instruments, the financial market regulation is not to be applied a priori. This first of all affects private payment tokens and “utility coins”, but in principle also all other tokens.



**Figure 11: Simplified presentation of the field of application of the financial market regulation**

Figure 11 shows that the areas of application of financial market legislation only make up a small part of the token economy.

The financial market legislation has clearly defined the publication obligations in the public sale of security tokens (pursuant to the WPPG), who can publicly issue security tokens as a service provider and what trading platforms are regulated.

As new innovative applications have become possible in the area of securities and in the environment surrounding currencies as a result of blockchain technology, specific questions are raised in this area on the applications of financial market laws with regard to tokens. A distinction must be made between two questions: Firstly, there is the question of how a company is treated that wants to offer a service which, in legal terms, is not a financial service, but nevertheless is connected with securities or financial instruments. An example of this is trad-

ing platforms where pure mediation of sale and purchase interests between private individuals takes place without the platform itself being involved in pricing, concluding trades or settling the transactions.

Secondly, there is the question of how a company is treated that wants to offer a service that is, functionally, a service comparable with a financial service but does not fall within this area of application due to the instrument in accordance with the current definition of financial market laws. An example of this are crypto-exchanges where payment tokens (“virtual currencies”) or “utility coins” are traded at high volumes which come very close to regulated securities markets (“stock exchanges”).

With this presentation, the government above all wishes to increase legal certainty across the spectrum of the token economy and, in particular, regulate the key service providers important to user protection and other interests of the state. With an essential regulation, all service providers in the token economy are given clarity and legal certainty regardless of which types of tokens they cover.

The discussion about the area of application of financial market laws to activities relating to the financial market is currently also ongoing in the European Union. The government is observing these discussions and will make the necessary adjustments where needed.

Figure 12 illustrates the regulation approach of the TVTG: The TVTG concerns the regulation of the bases for all applications of the token economy and not the treatment of applications relating to the financial market.

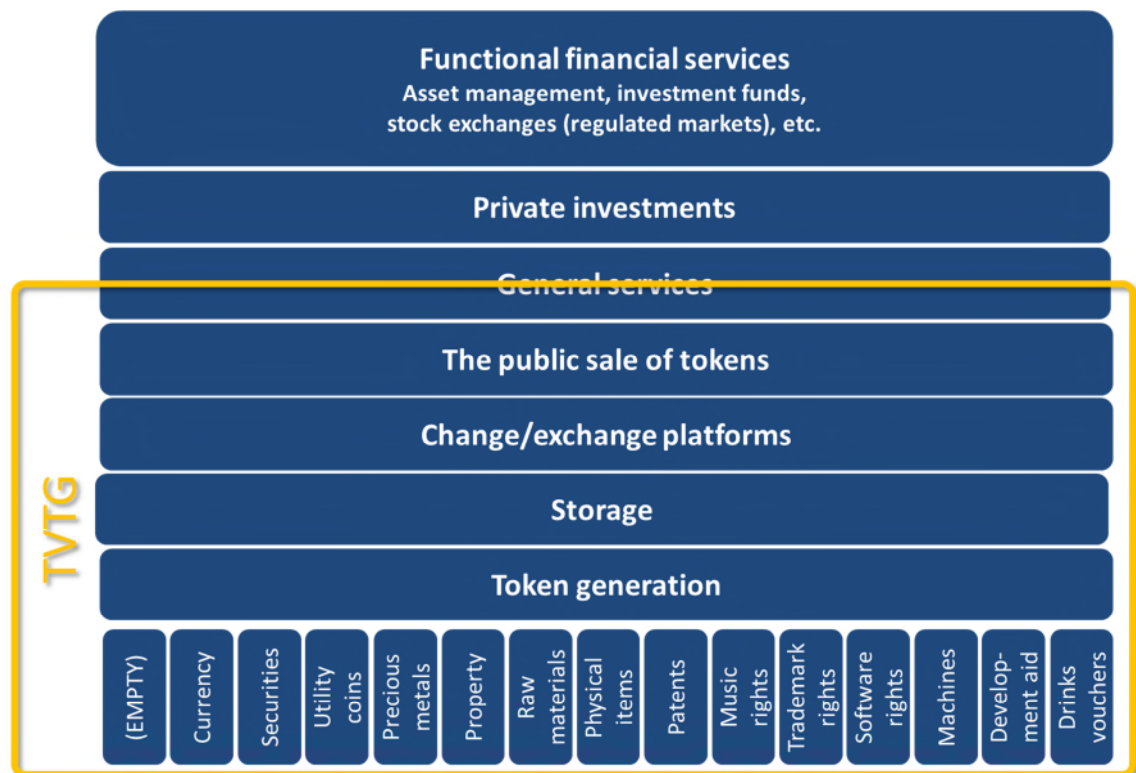


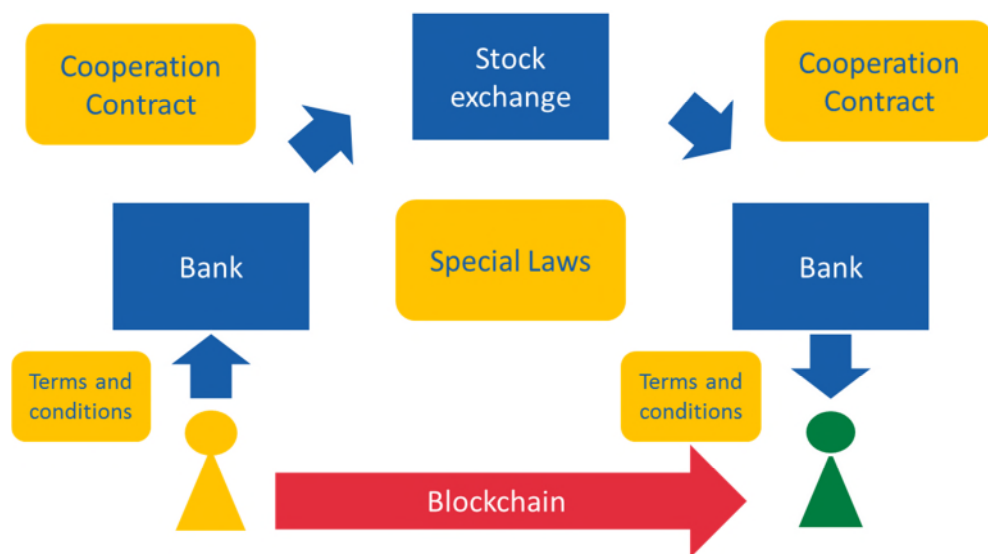
Figure 12: Illustration of the area of application of the TVTG

### 2.3.5 Efficient transactions and legal certainty as the basis for the token economy

The potential of the token economy is based largely on the ability to reproduce the “real world” digitally in a legally certain manner and transmit rights efficiently. The “technical” transaction costs constitute only a part of this efficiency. Another efficiency factor that a token economy requires is trust. A buyer needs to have confidence that he/she will effectively exercise the digitalised rights to a product or an asset and that he/she will be able to enforce his/her rights, where necessary with the aid of the rule of law. He/she also needs to have confidence in the companies and individuals who provide services on TT systems.

An analogy can be drawn here to the financial system: If an investor wants to buy stocks, for example, he/she will use a sophisticated and highly standardised transaction system which is guaranteed by the bank of the buyer and the seller,

brokers, custodians and an exchange, with a number of bilateral contracts, regulations and government supervision. This system allows a private investor to buy a stock with the click of a button in his/her e-banking account and have the confidence of knowing that he/she truly owns the stock and can exercise the voting and dividend rights. His/her rights in the event of the bankruptcy of an intermediary are also defined.



**Figure 13: Illustration of legal certainty of financial transaction systems in comparison to blockchain systems**

Transferring these “achievements” of the financial market to the token economy can accelerate its development substantially. However, in doing so it should be noted that blockchain technology generally is not made available by a single service provider, but is instead publicly accessible as a kind of digital infrastructure. Blockchain-based transaction systems are therefore more comparable with protocols such as the network protocol (TCP/IP), which enable the transmission of information over a decentralised network and thus provide the basis for professional services.

This results in the reasonable question of whether the blockchain protocol, the software itself or the programmers should be regulated in order to increase the

legal certainty for users. However, the government has come to the conclusion that such regulation of programmers would stifle innovation and is therefore not effective.

Instead there are two levels which are important for legal certainty: On the first level, there must be legal certainty for the “representation” of the “real” world in a blockchain system. Here the question of the classification of tokens plays a major role, as this transformation with regard to all aspects of the token economy is only possible with a suitable “token” model. However, this gives rise to new questions about the ownership of tokens and – based on this – to questions related to criminal offences and misuse, which must also be clarified legally.

Because the token economy can represent not only purely digital assets but also digitalised rights to physical objects or digitalised rights derived from contracts, the relationship between the digital representations in the tokens and the “analogue” rights must be clarified. The buyer of a token must be able to have the confidence that his/her legal position in relation to the analogue right or the real asset is clear. Especially with physical objects there is further legal uncertainty, as such objects can be transferred in an “analogue” manner without the knowledge of the “digital” owner. The right to a physical object can only be transferred efficiently if the buyer can be confident, without conducting an on-site inspection, that the object is actually available.

The second level involves the service providers which form a significant part of the token economy. A customer must be able to trust that the service provider is reliable and that their services are of high quality. While individual examinations by the customer might be generally conceivable, this would deteriorate the efficiency of the blockchain transaction system substantially. It is therefore much more reasonable to define basic requirements in terms of reliability and quality

through the government, as is the case with the financial market law, and require service providers to register and be supervised by the government.

Greater legal certainty at these two levels may help create an efficient ecosystem for digital assets and transactions and thus enable full exploitation of the potential of the token economy.

#### 2.3.6 Discussion in other countries

The development of blockchain/DLT-based innovations is being closely followed and analysed in most countries. However, the government measures and (legislative) proposals resulting from these analyses vary substantially from country to country. While some countries want to take advantage of the wave of innovation or see a need to act and therefore very early on devised laws or drafted laws, others have reacted differently. For example, in March 2018 the financial supervisory authority of Luxembourg published a warning against investments in crypto-currencies and ICOs. The following are examples as an illustration of the regulatory approaches taken by different countries:

Switzerland has taken up the subject of tokens and divided them into three different categories: Payment tokens, usage tokens and investment tokens. In December 2018, the Federal Council announced intended regulatory standards and opened the consultation process to improve the framework conditions for blockchain/DLT in March 2019. Key focal points should include creation the option of an electronic registration of rights which can guarantee the functions of securities, the segregation of “crypto-based assets” in the event of bankruptcy, the creation of a new category of approval for “DLT trading systems” in financial market infrastructure law and the option of acquiring an approval as an invest-

ment firm for the operation of an organised trading system. Current relevant practice should be refined as part of the fight against money laundering<sup>4</sup>.

Gibraltar has issued a DLT framework comprised of nine principles. Among other things, since 1 January 2018 all service providers which store or transfer assets on DLT systems for third parties require authorisation as a DLT service provider. This does not affect ICOs. DLT service providers must put measures in place to fight money laundering and financing terrorism in their operations that are adequate with regard to risk; in addition, suspicious transactions must be reported. DLT service providers are expected to be aware that their products and services may be attached with regard to risks associated with financial offences and must put measures in place to minimise these risks<sup>5</sup>.

At the beginning of 2018, Malta published three draft laws which address blockchain, crypto-currencies and DLT from a very technical perspective. In addition to the certification of DLT platforms, exchange platforms and trading platforms, the focus of these laws is also on how ICOs are conducted and licensed. The relevant laws came into force in July 2018. Service providers are therefore subject to the obligations to combat money laundering in accordance with the Virtual Financial Assets Act. White papers, which must be sent to the financial service authorities, must include a description of the procedure with regard to whitelisting and fighting money laundering and financing terrorism which must comply with the relevant laws<sup>6</sup>.

Bermuda passed an ICO Law in July 2018. This law only affects ICOs and token sales used for public crowdfunding or similar projects. Such ICOs need to publish

---

<sup>4</sup> [https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news\\_list.msg-id-74420.html](https://www.efd.admin.ch/efd/de/home/dokumentation/nsb-news_list.msg-id-74420.html)

<sup>5</sup> <http://www.gfsc.gi/dlt>

<sup>6</sup> <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/malta, section 5.>



a white paper and require authorisation. In connection with fighting money laundering and financing terrorism, company operating in the area of digital assets must establish appropriate internal rules and procedures. In doing so, they must comply with their customer-oriented obligations of due diligence, monitor business relationships on an ongoing basis, report suspicious transactions, manage relevant records and carry out internal controls and risk assessments; at the same time, compliance with rules and procedures must be monitored and ensured<sup>7</sup>.

## **2.4 Government objectives**

Digitalisation has for decades created significant momentum for the economy in general and for the financial services sector in particular.

The government is convinced that Liechtenstein's future prosperity and its ability to create an attractive range of jobs for the country and the region will only be possible through continuous development and entrepreneurial innovation. Because of the enormous number of regulations in the financial sector, private innovation requires a corresponding willingness to innovate on the part of the government and the authorities.

The government has therefore created structures for better supporting private innovation from the point of view of a liberal state. Particularly worth noting in this connection are "innovation clubs", a channel for the state innovation process, and the FMA's "regulatory laboratory". The regulatory laboratory functions as a contact partner for innovative companies in order to assist them with the approval process. By engaging in a dialogue with the practical field, in recent years the FMA has developed a good level of knowledge so it can make an in-

---

<sup>7</sup> [https://www.careyolsen.com/sites/default/files/CO\\_BER\\_Blockchain-and-Cryptocurrency-Regulation-2019-1st-Edition\\_10-18.pdf](https://www.careyolsen.com/sites/default/files/CO_BER_Blockchain-and-Cryptocurrency-Regulation-2019-1st-Edition_10-18.pdf), 6.

formed assessment of the opportunities and risks of new technologies and applications.

The openness of the government and the authorities towards innovation and new technologies, together with an in-depth dialogue with the practical field, have proven very successful in recent years. They have enabled Liechtenstein to develop a remarkable ecosystem in the FinTech space over the past few years. The concrete experiences and problems encountered in practice have, in turn, been integrated in the government innovation process and led to continuous small and large improvements to the state's framework conditions, and will continue to do so in future as well.

Against this background, the TTLA is a consistent part of these efforts of the government and the FMA to ensure optimal framework conditions. Many questions from current practice have gone into the drafting of this Law.

It is important to emphasise that blockchain technology and some applications already exist around the world as well as in Liechtenstein without a legally certain statutory framework being in place. For this reason, the government hopes the Law will clarify any questions that still remain open in order to create legal certainty for both users and service providers. Furthermore, it is very important for the government to protect users of blockchain systems against abuses and to preserve the reputation of Liechtenstein as a whole.

Because of the enormous potential that blockchain represents as a basic technology, the government has also decided not only to regulate current applications – in particular, crypto-currencies and initial token offerings (ITOs) – but also to create a legal basis for the much broader scope of application presented by the token economy. The aim of this approach is, firstly, to ensure that a new law does not have to be written for every new application and, secondly, to create

legal certainty for the many cases that are only now beginning to emerge in practice, but which are likely to develop in the near future. The government retains the right to specially regulate applications relating to the financial market in a further step.

This broad regulatory approach to the token economy largely corresponds to the feedback received from the practical field. Both blockchain companies and Liechtenstein financial service providers that provide blockchain-related services desire a clear legal basis in order to ensure greater legal certainty for themselves and to increase the trust of customers and users. The full potential of the token economy cannot be exploited without this trust.

In view of the enormous significance of the financial service sector in Liechtenstein, the government's aim in creating this framework law is to make it easier to bridge the divide between established institutions and blockchain applications. Blockchain technology will very likely become a potential and attractive basis for financial services (such as banks, funds, insurance companies and asset managers) as well as other sectors of the economy. It is therefore strategically important for Liechtenstein to address new business areas and the technology at an early stage in order to be able to take advantage of the opportunities that present themselves in this regard, as well as to reduce the risks discernible today from the point of view of the users and the state.

This Law is therefore a very important step towards creating good framework conditions in Liechtenstein for blockchain companies and the token economy. This step is part of the overarching state innovation process in which these framework conditions will be continuously developed. It must be expected that further questions will arise as a result of applying the proposed Law and developing the token economy. These questions shall be clarified on an ongoing basis.

## **2.5 The term “transaction systems on the basis of trustworthy technologies” and the title of the Law**

To prevent this Law from becoming outdated from a technical perspective and having a limited scope of application in just a few years, the technology-neutral formulation of the term “blockchain” is very important.

The term “blockchain” comes from the Bitcoin application and describes the serial logging of transactions in a distributed ledger and the block-based verification of a certain number of transactions. This makes clear that the term “blockchain” refers to a potential technical implementation. Although very well known among the public, it is not suitable as a technology-neutral formulation for the basis of this Law.

Another feature of blockchain systems is the decentralised storage of a single ledger for a large number of users (“distributed ledgers”). With the Bitcoin blockchain and many other blockchain generations, this is an important feature for ensuring manipulation security. However, it cannot be ruled out that in future blockchain systems will be developed without a decentralised ledger.

All current blockchain technologies are, as far as we can tell, based on cryptographic methods, i.e. encryption technology. This ensures that only authorised persons can access tokens and that transactions cannot be modified subsequently or only with substantial effort. However, because cryptography is used not only for blockchain systems but in nearly all areas of information technology, a term like “crypto-systems” is not sufficiently restrictive. In addition, it is theoretically feasible for procedures other than cryptography to be used for blockchain systems.

Another significant feature of blockchain systems is the absence of a central intermediary in the form of an organisation that is responsible for the integrity of

the ledger. With all known blockchain systems, it is only possible to dispense with the central intermediary because the integrity of the central ledger is ensured through technology and software-based rules. Security is based on technology and does not have to be ensured through a cumbersome and costly organisation.

The fact that trust is created by technology and not solely by organisations has tipped the scales in favour of using the term “trustworthy technology” as a connecting point for the Law. “Trustworthy” is understood to refer to the integrity of tokens which are clearly allocated and the secure exchange of which must be ensured.

Thus, the characteristics of blockchain systems described above are implicitly included: Many systems use cryptography, decentralisation and other rules in order to create precisely this sort of trust in the integrity of the main ledger.

The term “transaction systems based on trustworthy technologies” covers a view of blockchain systems that is as technology-neutral as possible in order to meet the needs of future technological generations as well. The government is therefore purposely choosing an abstract definition of the term “blockchain”.

The terminology should not be construed as implying that transaction systems not based on blockchain technology are untrustworthy. In the case of the financial transaction system, however, it is banks and all participants in the transaction network in the financial market which ensure that the system is trustworthy through organisational measures. By contrast, key bank software by itself is not trustworthy because, for example, bookings can be cancelled or deleted.

### **3. MAIN ASPECTS OF THE DRAFT**

#### **3.1 Explanation of the basic token model**

Today's blockchain ecosystem revolves primarily around payment tokens and its various applications (payment transactions, ICO). During the implementation of the ICO, it has also become clear that not only digital money, but also, for example, software usage rights or financial instruments can be represented on blockchain systems. This already makes it clear that a legal definition which is mainly about crypto-currency or crypto-shares cannot do justice to the full range of potential applications of the whole “token economy”. One therefore needs a more abstract formulation that goes beyond “money” and “securities”.

In order to be able to cover as many possibilities of use for the token economy as possible, they shall be associated with rights. Everything that is used in the legal and economic system can be subsumed under this term. Thus it can include the right to purchase Swiss francs, the legal title to a property, the right to purchase goods (vouchers), usage rights of all kinds, rights of lien, payment and membership claims and much more.

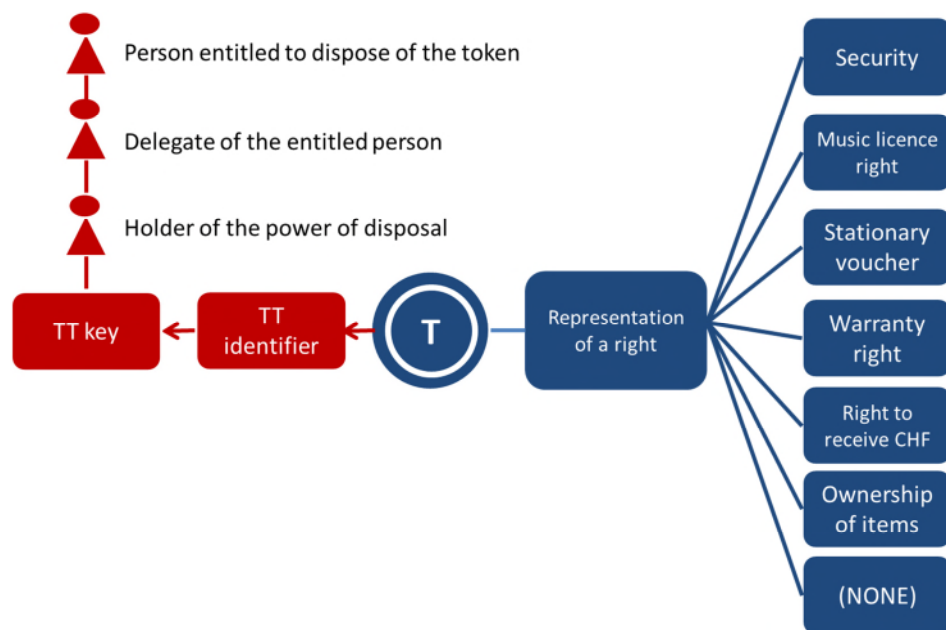
This logically means that these rights are just represented in digital form on TT (Trusted Technologies) systems, or are subject to the legitimation and transfer regulations of the TT system. The original “legal right” and thus all the related legal consequences remain in effect. For this representation of rights on a TT system to have legal certainty, this Law introduces the legal subject of the “token”, which makes it possible to represent all types of rights on a TT system in the first place. The “token” is therefore a kind of “container” for representing a right. The case of an “empty” container is also possible, and relevant in practice, for example crypto-currencies without real value collateralisation (e.g. Bitcoin). In fact the model chosen in this Law can also cover a large number of other ap-

plication cases (e.g. ownership or usage rights to property, intellectual property rights, warranty rights). Here one must remember that there are already many different technologies which are grouped under the term “blockchain”. The legal definitions in this Law are deliberately formulated in as technology-neutral a way as possible in order to be suitable for future technological developments.

With the introduction of this new legal object (token) in Liechtenstein law, various questions must be clarified such as rights to tokens, delegation to third parties and the legal connection between the token and the represented right.

This Law therefore introduces the following basic model (see figure 14):

- the “token” as a new legal object for representing rights of all kinds,
- the “TT identifier” as an element to assign tokens (a type of unambiguous “address” in blockchain systems derived from the “public key”),
- the “TT key” as an element to dispose over tokens assigned to a “TT identifier” (named “private keys” in blockchain systems),
- the “holder of the TT key” as a person who can actually dispose of the “TT key”,
- the “person possessing the right of disposal over the TT key” as a legal person entitled to rights similar to those of an owner of tokens, and
- the “delegate of the person holding the right of disposal” as an independent role, for example, in the case of safekeeping of TT keys.



**Figure 14: Illustration of the basic token model  
used in the Law and various roles**

This basic model is necessary to provide a legal basis for all possible application cases that may be found in practice. The individual elements are described in more detail in the following sections.

## Token

As already mentioned, the “token” will be introduced as a new legal object to represent rights of all types on TT systems. A token can represent rights such as payment claims (certificated or uncertificated) against a debtor, membership rights in a company, property ownership rights or limited rights in rem to movable property (e.g. diamonds or works of art) or immovable property (real estate), or indeed other rights such as intellectual property rights. The basic model – as already mentioned – also permits of empty containers, i.e. tokens without represented rights. An example of this is crypto-currency such as Bitcoin, which only accrues an intrinsic value through the rules of the system in order to function as a means of payment.



Because tokens only serve to represent the rights to real assets (as a collective term for real rights of all kinds), it is clear that the creation of tokens does not create a new right, but only subjects an existing right to the transmission and legitimisation system of the blockchain. If the container holds some content, the right is transferred according to the rules of the blockchain (transfer system). In the case of claims, those persons who are legitimised according to the rules of the blockchain are also considered legitimate in relation to the debtor.

In line with the objective of ensuring neutrality in terms of technology, the term “token” is understood abstractly in this Law and not technically. This means that the legal definition of the “token” is taken to mean every connecting point of rights on a TT system, regardless of whether they are technologically implemented as a “token”, or whether the token is “filled” or not. This is important because already now there are TT systems which have chosen to use other forms of technical implementation. In the case of Bitcoin for example, the “digital coin” or token is technically seen as a fraction of a Bitcoin which is allocated to an address in a kind of decentralised accounting system. Nonetheless, the regulations on the disposal of tokens should still also apply to Bitcoin in order to ensure legal certainty.

The introduction of the new legal element of the “token” also requires that the legal consequences must be defined. In particular, the definition of rights to and the transfer of the token, and the legal consequences of the relation to the represented right, play important roles here.

The abstract definition of the “token” as an independent legal object used to represent any right requires that one or more persons may have rights to the “token” and transfer it legally to other persons. With regard to rights to tokens, tokens certainly bear similarities to an item of property, i.e. a physical object. However, the concept of ownership of an object, which is defined in the 1923

Property Law (SR), is basically limited to physical objects. Since a token technically only represents information or an entry in a TT system, i.e. it “only” consists of digital character strings, it is clear that a token has no physicality. It would therefore not be right to use the property law concept of ownership here and that would lead to legal uncertainty. Theoretically, it might be possible to extend the property law concept of ownership beyond physicality and declare that it can also be applied to tokens. This would, however, require deep inroads into property law, as many provisions would have to be rewritten. One would have to consider the legal consequences very carefully, because property law not only regulates ownership of property, but also real estate, limited rights in rem such as easements and burdens, as well as mortgages and so on.

The government has therefore decided to autonomously regulate ownership of the token and the associated legal consequences only for TT systems. This does not affect the established system of property law and creates a clear and well laid-out legal framework for tokens in relation to TT systems, which can also be understood by non-lawyers. For the very same reasons, Switzerland has also opted for an autonomous regulation in its Intermediated Securities Act (*Bucheffektengesetz*), with the development of a legal concept *sui generis* (the intermediated securities) in its reform of custody account law. However, it should be emphasised that the situation is different in the case of TT systems, because here one does not find the highly complex and multi-tiered relationships that prevail in custody account law. Instead, a direct assignment of assets to their legal entities is possible at any time. Just as in intermediated securities law, however, specific questions present themselves in TT systems as a result of the fact that real assets such as rights are represented on a TT system (duality of assets). Traditional property law provides no answers to these special features.

The autonomous regulation of token rights in the TVTG does, however, require that independent concepts or terms be created. For this reason, this Law introduces the concept of the “person entitled to dispose of the token”, as well as the “holder of the power of disposal of the token”. The person entitled to dispose of the token may legally dispose of tokens and is considered as the owner of the token and therefore also as the legal holder of the right represented in the token. According to the current state of knowledge, however, disposal of tokens cannot be exercised directly for the most part, but only by way of the private key. This means that a duality exists in the right of disposal over a token and over the TT key. This is why the right of disposal under this Law is linked to a TT key. Whoever knows about the private key is also the “holder of the power of disposal”, although this does not necessarily have to be the person entitled to dispose of it (see the explanation about the “TT key”). The independent definitions of the “person entitled to dispose of the token” and the “holder of the power of disposal” that are made in the Law are of central importance particularly for TT systems in order to operate services in a legally certain manner and avoid misuse.

Another central challenge of the TT transfer rules to take into account the duality of digital and analogue assets in such a way that legal certainty is ensured both online and offline. Legal certainty online means that the purchaser of a token must be certain that he/she also acquires the right associated with the token. Legal certainty offline means that persons who acquire an item or a right offline are not exposed to the risk of being left empty-handed in relation to buyers of the corresponding token. Both requirements – legal certainty online and offline – are essential conditions for a legal framework that enables the transfer of assets.

Legal certainty online can be ensured by the TVTG determining that disposal over a token has the simultaneous effect of disposal over the represented right. In the interest of legal certainty and clarity, it should also be made clear, regarding the

individual categories of representable assets (objects, receivables, etc.), that disposal by means of tokens is possible. However, such a clarification in a Liechtenstein Law can only have an effect on assets that are subject to Liechtenstein Law (e.g. a movable object located in Liechtenstein).

As a structural measure to ensure the synchronisation of digital and analogue disposal, the Law therefore imposes the obligation on the Token Generator that he/she ensure by suitable measures that disposal over the token actually brings about direct disposal over the represented right as well, and that any other disposal over the right represented in the token is excluded.

The Law does not specify in detail how the Token Generator is to fulfil this obligation. If a token is to represent a right to a movable object (e.g. diamonds), the owner of the physical item will have to deposit it, for example, at a warehouse. In the case of securities, it should usually suffice if the terms of issue stipulate that disposal over the securities is subject to the rules of a TT system. It is also to be expected that further technical solutions will arise as the technology develops.

The token model can be extended. For example, it is possible to represent rights to a token in another token. Examples of this are derivatives, property usage rights (e.g. apartments, cars). It is also possible to represent the rights to so-called wallets in tokens, such as administrative rights or rights of lien, in order to simplify the digital rights transactions between customer and service provider. Fund unit rights can be issued in the form of tokens and allocated to the investor's wallet.

From a technical standpoint it is also possible to represent software code in tokens (function tokens). This may indeed be of interest from an application point of view, but from the government's point of view there is currently no particular

legal uncertainty in this form of use such as one finds with the representation of rights and assets in tokens. Therefore these other applications are currently not included. The government reserves the right to place further applications of the blockchain under the protection of the Law should this prove necessary at a later date.

### **TT identifier**

The roll of a “TT identifier” is required for assignment to users on TT systems. It is usual for a number of tokens to be assigned to a single TT identifier. The TT identifier thus plays a central role in the transmission of tokens between users. Wallets therefore always consist of one or more TT identifiers to which and from which tokens can be transmitted.

TT identifiers are generally assigned to a person. This may be, for example, the person entitled to dispose of the token, or also service providers such as the TT Protector, who assigns the tokens of customers to one of its TT identifiers.

TT identifiers can also be assigned to machines (Internet of Things). In this way transactions can also be carried out directly with machines. An example of this can be found in car-sharing models where the right of use is transferred and payment is made directly via a TT system.

“Smart contracts” are another possible way of assigning TT identifiers. Smart contracts are automated policies that can also initiate transactions with tokens.

### **TT keys**

Another central element is the so-called “TT key”: Disposal over a TT key can be gained de facto by way of the tokens allocated to the associated TT identifier.

The TT key thus has a very important role in creating legal certainty on a TT system.

The TT key holder therefore has the actual power of disposal of the token. Yet the holder need not be the person possessing the right of disposal. If a third party acquires a private key without authorisation, the third party gains de facto power of disposal over the token and can therefore initiate transactions. But from a legal point of view he/she is not entitled to dispose of it.

Consequently, a distinction is made in the Law between the holder of the power of disposal and the person possessing the right of disposal. To ensure that the applications are practicable on TT systems, the Law irrefutably assumes that the holder of the power of disposal is also the person entitled to dispose. In the event of unauthorised acquisition, this assumption can be refuted.

The person entitled to dispose of the token may delegate rights of disposal in whole or in part to a deputy. In doing so, the deputy also becomes the person possessing the right of disposal over the token but is restricted by his/her mandate in the internal relationship. This authorises the deputy, for example, to initiate a transaction on behalf of the person entitled to dispose of the token.

In practice, the delegation is often made to a TT key depositary. The TT key depositary keeps the TT key on behalf of the customer, for example, to better protect it from misuse. Thus the TT key depositary has the de facto power of disposal over the token and also the authorisation to store the TT key. This gives him/her a limited power of disposal. Another form of limited power of disposal is the right to initiate transactions on behalf of the customer.

It is technically possible to copy TT keys. The owners of the copies will then have the de facto power of disposal over the token. In contrast, only the rightful owner of the token is actually entitled to dispose of the token. Transactions initiated

by those who hold the copies are not legal and may be contested by the person who is entitled to dispose of the tokens.

It may also be possible for the TT identifier to be accessed via several TT keys. This means it is technically feasible to regulate collective signatures. The model used in the Law allows for such applications.

The distinction between the holder of the power of disposal and the entitled person is also important when it comes to the use of machines and smart contracts on TT systems. As explained above, machines or smart contracts can be represented in a TT system by TT identifiers. This means that tokens can also be assigned to them, which they can dispose of using TT keys. So a machine or a smart contract can have the power of disposal, and the persons behind it can have a delegated right of disposal via a deputy.

## **Disposal**

The disposal transaction is the legal transaction by which a right is transferred, encumbered, amended or revoked; in addition to the transfer of the right of disposal, it also includes the creation of a right with limited rights in rem (for example a lien or usufruct).

Disposals are not effective unless the person possesses the right of disposal, i.e. is entitled to initiate the change in legal status at issue. This results from the logical legal principle that no one can transfer more rights than he/she has, which undoubtedly also applies to the disposal of tokens. The right of disposal to the token comes close to the right of ownership to a physical item. This right can be granted to a third party by law or by legal transaction (representation as deputy). The right of disposal can be withdrawn; this is particularly the case when bank-

ruptcy proceedings are opened with regard to the assets of the common debtor (Art. 15 para. 1 Bankruptcy Act).

In the context of disposal of tokens, the prerequisite of power of disposal seems to be unproblematic insofar as only the holder of the TT key has the power of disposal over the token and can thus trigger the effects of disposal. If the holder of the TT key is also the person entitled to dispose of the token, he/she can also authorise another person to dispose of this token to which he/she is entitled, in accordance with the general rules of representation. In all these cases, the nominal legal situation and the factual, validated situation according to the blockchain are aligned and match up.

By contrast, there may be a discrepancy between the nominal legal situation and the factual situation, for example, if the holder of the TT key has bankruptcy proceedings initiated, and he/she then makes a transfer which is validated and thus concluded in accordance with the rules of the system. In such cases, it is possible to refute the legal presumption that the holder of the private key is also the person entitled to dispose of the token.

The inalterability of transfers to TT Systems suggests that the principle of abstraction should be posited for dispositions of tokens, meaning they are also to be considered valid even if a valid obligation-creating contract has not come about (e.g. on account of unlawfulness) or has been subsequently rescinded (e.g. due to a challenge invoking an error). The principle of causality would here lead to a discrepancy between the nominal legal situation and the actual, practically unchangeable circumstances documented on the TT system. This does not mean that disposition is final and absolute but rather only that it is to be reversed in accordance with the law of enrichment in that the unduly enriched purchaser transfers back the tokens, by way of a new transfer procedure, to the person



unduly deprived of the tokens (or is possibly forced to do so by virtue of a court judgement).

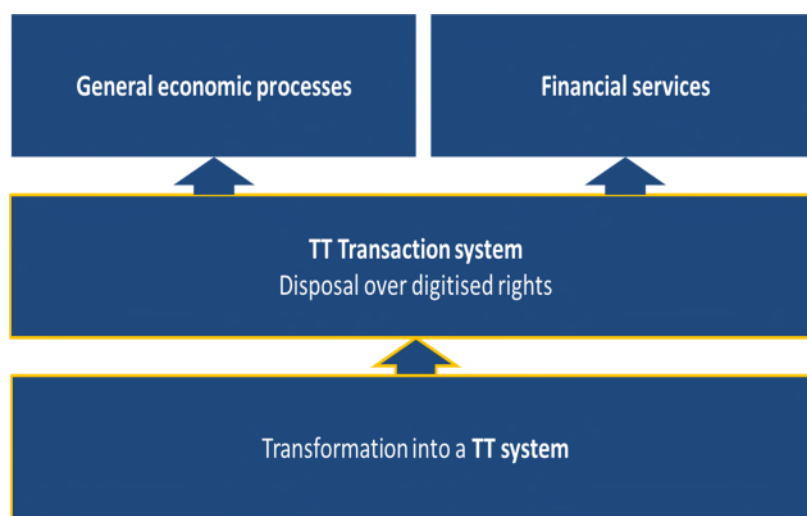
It should be noted that the Law can only regulate the right to dispose of and transfer the token. The effects that a transfer of tokens has on jurisdiction for the represented rights are only covered by Liechtenstein Law insofar as they are subject to Liechtenstein Law under the rules of Private International Law (IPRG). Different rules concerning conflict of laws apply, depending on the type and legal nature of the represented right. Movable property, for example, is only subject to Liechtenstein Law if it is located in Liechtenstein (at the time of disposal).

Even tokens that do not represent rights will require rules about their legally binding disposal. In this context it is clear that the rules on disposal of tokens can also be applied analogously to “empty” tokens, in order to provide the necessary legal certainty here as well.

## 3.2 Activities on the TT system

### 3.2.1 Transformation into the TT system

As the following illustration shows, TT systems not only enable direct transactions between persons, but can also provide the basis for all types of economic services and processes, in particular also for financial services.



**Figure 15: Schematic overview of the levels of the token economy**

A token economy is therefore essentially based on legal certainty in the TT system and the legally defined transformation of the “real” world into the TT system. The first step in the process chain to represent a right on a TT system is the creation of a token and the representation of this right in the token. Here the token generation is not necessarily bound to the development of a new TT system, but is defined as an independent activity from the legal standpoint. On the one hand, the creation of a token requires programming skills; on the other hand, the representation of the right, and the rules governing how a token can be transmitted, must be correctly represented in technical terms pursuant to the rules of this Law.

To ensure the legal certainty that is required in a token economy, and the buyer's confidence in the quality of a token, in future the work of token generation will increasingly be provided by professional service providers. Therefore the Law legally defines the role of "Token Generator", which also clarifies the distinction from "Token Emission".

The role of the "token generator" is essential for the token generator as the purchaser's trust in the functionality of the token can be greater, therefore waiving the need for the otherwise necessary verification tasks before the token is purchased. Customers should have a greater degree of trust in the services of token generators as a result of government registration. This is also helpful when it comes to integration within other services, such as funds, stock exchanges and so on, in order to encourage outsourcing and thus accelerate the development of a specialised ecosystem.

In the government's view, there is a special need for protection in case of a representation of rights to property. With rights to property there is a duality between "online" and "offline", i.e. between the tokens and the real objects. For legal certainty and credibility of the token economy, it is essential that the buyer of a token can be sure that the object or item actually exists. Conversely, a buyer of an item must know that the rights to the item are registered on a TT system, and a transfer of rights can only be legally valid on the TT system. Encumbrances or charges, such as rights of lien, must also be recognisable in both the digital and analogue worlds.

The government is therefore introducing the role of the "Physical Validator". The main function of this is to ensure the connection between the object and the token that represents rights to it. To more clearly explain the concept behind this role, some specific examples will be described in concrete terms.

In the first case, the legal title and right of lien for a physical object of value (e.g. a diamond) is to be represented in tokens. The object of value is stored in a warehouse. A token generator now generates the two tokens, while the physical validator ensures the following:

- a) Identification of the object of value (serial number, certificates, etc.);
- b) Storage location, storage conditions (e.g. securing the access);
- c) Identification of the client and ensuring that the client is also the lawful owner of the object of value;
- d) Avoiding conflicts of rights: The main issue here is that the object of value is not already encumbered “offline”, e.g. by liens.

The physical validator must also ensure that the duties of the warehouse are contractually regulated, i.e. so that no one may have access to the object of value without the legitimization of the token. Only the person authorised to dispose of the token may remove the diamond from the warehouse with the knowledge of the physical validator, provided all the associated tokens have first been cleared at the same time. This also protects the rights of all other token holders who have acquired rights to the object of value.

The associated storage agreement between the physical validator and the warehouse must also stipulate that no further rights to the object may be established without the agreement of the physical validator. In particular, further liens may only be created with the knowledge of the respective physical validator.

The second case deals with a valuable watch: When a watch is manufactured, the manufacturer arranges for a Token Generator to create tokens with the legal title, lien, warranty and usage for the watch. The physical validator ensures that the serial number and original certificates are correctly recorded and match the

watch. When buying the watch, the purchaser also takes over the tokens with all the rights. This allows him/her to prove at any time that he/she is the rightful owner of an original watch. He/she may then also pass on these tokens individually, for example, to obtain liquidity. To do this, he/she assigns the lien token to a liquidity provider with the right to use the watch if debt repayment is not complied with. The question now arises, for the liquidity provider, as to whether the watch will really be available should he/she seek to use it. The watch could have been stolen, or it could have been sold on by the bearer without notifying him/her. To cover such cases, the physical validator concludes a contract with the bearer or owner of the watch, in which the obligations of the bearer are regulated, for example, the type of insurance the bearer must take out (e.g. against theft). Should the watch not be available at the time when the liquidity provider wishes to assert his/her pledge, the physical validator is primarily responsible and has to ensure that the financial claims of the liquidity provider are quickly satisfied. This special responsibility is of greater importance in a TT system, because the contractual partners may not know each other directly, and so they can only draw the full benefits of the token economy if the purchaser can be sufficiently confident as to its workings. The physical validator, on the other hand, must enforce his/her claims against his/her client under civil law.

Since this pivotal function of the physical validator is very central to user protection as well as for other reasons, it is stipulated that this role requires registration.

There are certainly a number of other use cases in the token economy besides the right to property, for which a similar pivotal function might be necessary, e.g. for copyrights or general contracts. The government reserves the right to introduce further roles in response to corresponding feedback from the private sector.

### 3.2.2 Types of delegation

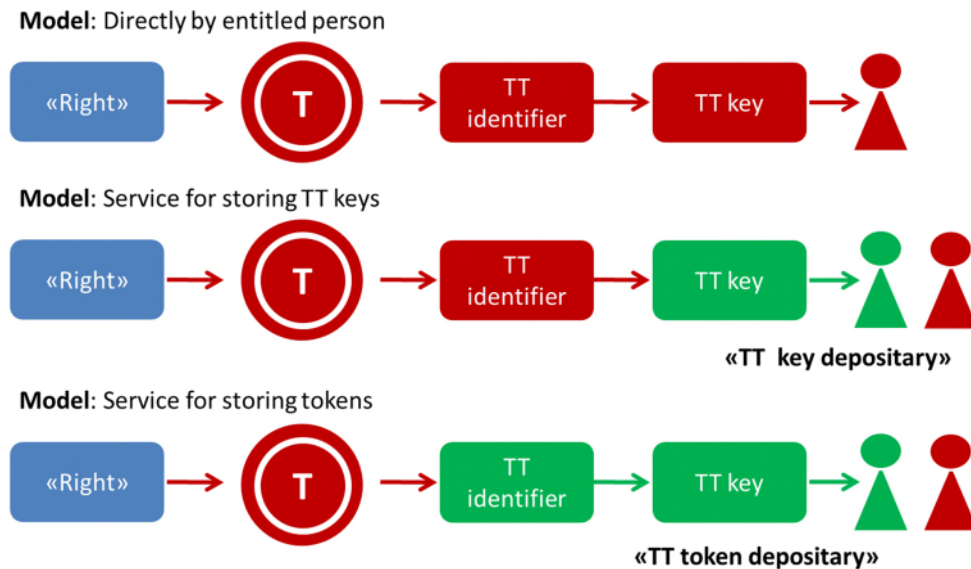


Figure 16: Illustration of the delegation models

As described above, tokens on TT systems are typically assigned to an address, generally known as the “TT identifier”. All the tokens that are assigned to a “TT identifier” can be disposed of via the “TT key”. This also means that the loss of the TT key has major consequences in that no-one can dispose over the token any longer (“ownerless 2.property”) or an unentitled third party can misuse the tokens, for example by transferring them to another “TT identifier”. It should be borne in mind here that TT keys cannot be restored if they are actually lost, according to the current state of technology, nor should they be, because otherwise one could no longer guarantee the security of the TT system. This means that tokenised rights in assets are lost to heirs if the decedent did not make any backup copies of his/her TT keys or the decedent's TT keys cannot otherwise be made accessible upon his/her death. Today there are a number of professional service providers who offer various types of custody in order to ensure the greatest possible security for specific application cases. The storage of TT keys in a mobile wallet is more like an actual “wallet” with the same consequences in the event of theft.

There are basically two models for the delegation of custody to TT service providers: In the first model, the TT key is entrusted for secure safekeeping by transferring it to a TT identifier managed by the depositary, and in the second model the token is entrusted to a service provider.

#### Role of the TT key depositary

The TT Depositary keeps TT keys on behalf of clients in order to ensure a higher level of security, or an easier disposal as part of their services. In technical terms, the TT key depositary will in most cases generate the TT key directly for the customer, otherwise he/she cannot exclude the possibility that there may be several copies of the same TT key in circulation. Typical examples are:

- a) Wallet providers that store the TT key centrally on a server, thereby reducing the risk entailed by a possible loss of the smartphone.
- b) “Offline storage providers” who store TT keys separate from the Internet in order to reduce the risk of hacker attacks.
- c) “Crypto-exchanges”, which initiate the disposal of the tokens directly on behalf of the client via the TT key, allowing trading transactions to be carried out more efficiently.

From the user's point of view, delegation leads to a risk of the misuse and loss of assets, especially in the case of bankruptcy of the service provider, or if the technical precautions are not sufficiently robust. With this Law the government protects the user by requiring that the tokens that can be disposed over by TT keys must by law be kept separate from the assets of the TT key depositary in the event of bankruptcy and they must not be used to satisfy creditors' claims. Such

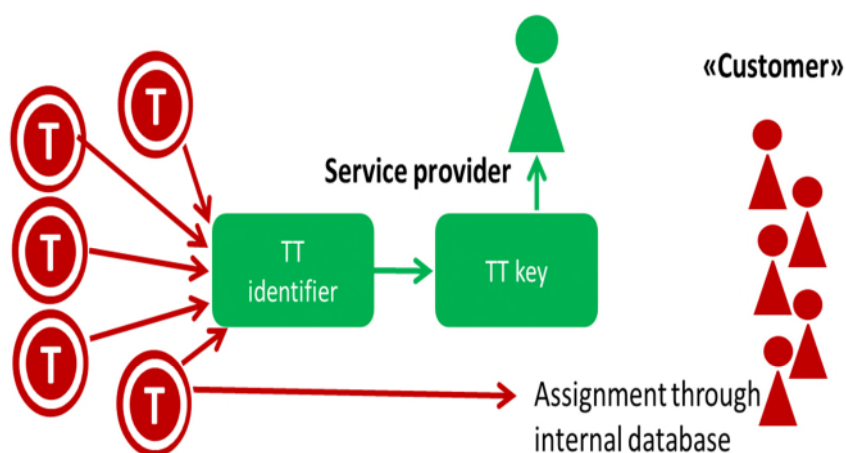
a regulation exists for securities portfolio accounts with banks and investment firms and is an essential element in ensuring legal certainty.

Further, the government protects the user by formulating a minimum standard for TT key depositories, which also takes into account their internal procedures. This is to strengthen user confidence in TT key depositories.

Unless provided for otherwise by way of *lex specialis* stipulations, the provisions of the General Civil Code (ABGB) pertaining to custodian agreements apply.

#### Role of the TT token depository

The token safekeeping service for customers is rendered by the role of the TT token depository. The TT token depository is of practical relevance in some applications. Firstly, this role is important for transaction accounts. Transaction accounts are used, for example, by crypto-exchanges, custodian banks, etc. to efficiently process a large number of transactions by many customers. The TT token depository shall assign all of their customers' tokens to one or several TT identifiers over which it has the power and right of disposal. The allocation to the customer is done in a – usually separate – database.





**Figure 17: Illustration of the “TT token depositary” model**

### 3.2.3 Token issuance

The Law deliberately makes a distinction between the generation and the emission of tokens, even though in today’s applications in the form of Initial Token Offerings (ITOs), Initial Coin Offerings (ICO) and Token Generating Events (TGEs), tokens are often offered directly to the public when they are generated. In view of the wide range of applications of the token economy, this will still be rather a special case, while the actual representation of rights in a token can be used much more widely. Tokens can also represent individual rights to items of property of private individuals and do not necessarily always have to be offered to a large section of the general public. In this context it is important to emphasise that all types of tokens are involved here, and not just payment tokens or so-called utility coins (for example, as a type of software usage right).

The Token Emission therefore concerns the initial public offering of tokens and is independent of whether the tokens were generated during or before the emission, and whether the emission is carried out in one’s own name or in the name of a third party. The public character, i.e. the sale of tokens to a large circle of people (the general public) who are not personally known to the person, also features in the special protection of purchasers by the TVTG. The processing of an emission, i.e. the exchange of tokens (e.g. payment tokens vs. new tokens), involves a certain risk of abuse. Accordingly, the government stipulates the following measures to strengthen legal certainty in the emission of tokens:

Firstly, the process of token emission in Liechtenstein will be subject to registration under the TVTG. Token Issuers are therefore subject to the legally specified minimum standards for TT Service Providers, and must also ensure appropriate internal procedures for the proper execution of a Token Emission.

Secondly, Token Issuers are obliged to publish basic information about the tokens and to correctly inform potential buyers about the tokens.

According to the requirements of article 30 et seq., an issuer of tokens that are offered to the public is obliged to prepare and publish appropriate basic information in advance. The corresponding obligation to provide information serves the protection of users, and is intended to duly inform the interested public about the purpose of the Token Emission as well as the associated opportunities and risks.

The systematic structure of this article is based to a large extent on the provisions of the Securities Prospectus Act (WPPG). The provisions of the WPPG (e.g. definition of terms) can therefore be used as an additional resource for the interpretation of article 30 et seq.

The main difference between a securities prospectus under the WPPG, and basic information under the TVTG, is that although the latter must be submitted to the FMA in good time before the token issue, and the information must also be published, e.g. on the issuer's website. However, no formal approval of the information is required by the FMA.

Another important difference between the WPPG and the basic information under the TVTG is that buyers of tokens are not necessarily investors who buy tokens primarily for the yield they can obtain. Because tokens can represent all kinds of rights, the formulations in article 30 are worded in a more general way so that they can also cover applications other than investments.

When introducing an obligation to publish basic information, the legislator must be aware of this very broad range of applications. At present, discussion extends primarily to initial coin offerings (ICOs), which include the issuing of tokens to finance projects. The publication of basic information makes sense for most of

these ICOs and is also expected by users. In a token-based economy, however, there are a wide variety of advanced applications of token issues including those for which the obligation to publish basic information does not appear appropriate. An example of this is beverage vouchers for large public events. Although applying a TT System would make sense, the risk posed to the consumer of not being able to redeem a beverage token is comparatively small. And presumably, the users would hardly be willing to read the basic information at all.

With the obligation to publish basic information and the regulations on content, the government wishes to make it clear that providing correct information for buyers is important for legal certainty. Yet it seeks to word the exemption clauses in an open manner so that the many applications which also require the legal certainty of this Law, but which would be rendered impossible by excessively heavy-handed regulations, are also possible. Ultimately, the government relies on the users' own sense of responsibility to check that they have been adequately informed before buying tokens.

The objective of the Law is to regulate those persons who offer tokens to the public, so as to ensure the protection of users and to allow the Financial Market Authority to perform its supervisory function. The TVTG does not intend to cover persons who trade their generated tokens with other persons out of the public view (over-the-counter, OTC).

So-called "mining", i.e. the verification of transactions on TT systems, is not seen as a Token Emission according to this Law, since these tokens are not usually offered publicly, but are personally assigned to the "Miner" as compensation for his/her service.

### 3.2.4 Other service providers

#### TT Price Service Provider

In addition to the roles introduced above, other specialised services will also be developed on TT systems that do not all require special protection under the TVTG. There are some, however, which are particularly sensitive – just as we find on the financial market – and should be officially registered by the government in order to create user confidence and prevent abuse.

Such a service is for example a trading or exchange platform on which a number of users buy and sell identical tokens. Exchanges on TT systems differ significantly from traditional stock exchanges: The TT system itself ensures the complex internal organisation that is needed in order to reliably execute securities transactions. The custody of securities is already covered by the roles of the TT key depositary and the TT token depositary. So at present there is no need for additional regulation of this aspect by the TVTG.

Ultimately, there is still the service to calculate and publish aggregated prices on the basis of transactions and offers. Since this activity is very important for the protection of users and other service providers, to avoid abuse and insider dealing the government defines this activity within the context of the role of “TT Price Service Provider”, and does not regulate a “TT exchange” as such but rather favours the modular registration approach.

#### TT exchange service providers

Legal tender such as Euros or Swiss Francs are exchanged into payment tokens on TT systems via TT exchange service providers.

### TT Identity Service Provider

Establishing an identity is of great importance for legal certainty on TT systems. During the transfer of tokens to another person, or the assignment of a service provider, it is essential that the counterparty is reliably identified.

This service is also essential for the integration of machines (Internet of Things). In this way, users who are carrying out transactions with machines are able to check beforehand who these machines are assigned to. This functionality can, for example, be applied to car-sharing companies, where a user pays for the service directly via the TT identifier of the car, which could then unlock itself.

### TT Verifying Authority

When transferring tokens, the specific legal regulations must be observed. On TT systems, the transmission of tokens mainly takes place without personal contact. To ensure that the efficiency of the TT systems is not hampered by having to comply with the legal requirements, the role of a TT Verifying Authority will be created, which checks these prerequisites for disposal. Usually this is done by a software.

### 3.3 Regulatory approach

When regulating TT systems, the basic question arises as to whether the technology can or should be regulated itself. Due to the high pace of innovation of TT systems, and the lack of a regulated intermediary, it does not make much sense for the government to regulate the technology itself at this point in time. Adequate regulation and supervision of the TT service providers themselves is therefore called for, whereas the critical technical examination of the TT systems on which TT service providers offer their services must be carried out by them themselves. For TT service providers, it is therefore not only possible to quickly react to various developments on TT systems (e.g. forks<sup>8</sup>), but rather they are legally obliged to do so (see article 29(1)(b) TVTG).

As explained in Section 2, there are risks for users of TT systems that are known from current practice, which the government intends to reduce with the present Law. Section 2 also explains that there are new application scenarios on TT systems regarding money laundering and criminal abuse. Beyond meeting the registration requirements, it is therefore important that TT service providers in the area of the SPG (*Sorgfaltspflichtgesetz* - Due Diligence Act) are supervised.

As mentioned in section 2.3, any applications of the token economy already fall under the applicable financial market legislation. In these cases, many question on user protection, combating money laundering and supervision have already been clarified and do not currently require further regulation under this Law. However, these intermediaries must have sufficient expertise regarding the specific features of TT systems in order to provide high-quality services of the same

---

<sup>8</sup> Splitting of a TT system, for example, by continuing with two copies of the same blockchain under different rules. A well-known example is the splitting of the Ethereum blockchain, so that two TT systems are now continued as Ethereum and Ethereum Classic.

value with regard to tokens and TT systems in comparison to the traditional financial market infrastructure.

In contrast, the need for regulation is far greater with regard to applications and TT services which are not covered by financial market supervision laws.

With the TVTG, the government is therefore introducing minimum requirements for all TT service providers in Liechtenstein, which are important from the point of view of user protection, compliance with international standards and the protection of the reputation of the country. Even if there are more and more applications relating to the financial market today (e.g. crypto-exchanges), the TVTG is a system of regulation that should apply to all forms of the token economy. This also includes the simple applications of tokens, e.g. a drinks voucher for a festival. The government retains the right to specially regulate applications relating to the financial market in future in addition to the TVTG.

The government based the choice of this system of regulation on the account information service provider that will be regulated with the implementation of PSD II in the Payment Services Act (ZDG).

Persons with headquarters or place of residence in Liechtenstein that wish to render professional TT services in Li must register with the supervisory authorities in advance. Companies with headquarters abroad may not in general be subject to Liechtenstein regulation. If a foreign company sets up a physical change machine (e.g. a Bitcoin change machine) in Liechtenstein, this is considered a special case. The physical presence in Liechtenstein is the basis for being subject to the requirements of the TVTG and therefore also the SPG.

The obligation to register as a TT service provider requires the “professional” exercising of the TT service in question. The government therefore wishes to exclude private applications of blockchain technology regulation. This demarca-

tion is important as blockchain technology can be used in a very large context, such as managing the supply chain in industrial operations or issuing drinks vouchers at a festival without the customer requiring special protection. In light of the foregoing, whether or not the TT service provider performs its activity in exchange for a fee is essential for interpreting the term “professional”. Furthermore, users must be protected if the TT service provider intends to provide its services to a large sector of the general public in an undetermined number of cases. Professional performance cannot be assumed if a service is rendered as a courtesy and the trust in the TT service provider is not based on the personal close relationship with the user, but on other characteristics of the TT service provider (specialist skill, reputation, etc.). For example, a company using tokens to issue food vouchers in a work canteen for employees does not constitute a professional service and does not require registration. Likewise, a bookshop that issues gift vouchers via tokens does not require registration. The generation of tokens forms part of its commercial activity that it performs for itself and not for third parties in exchange for a fee. Only if bookshops were to create tokens in exchange for charging a third party would the token generator need to register as a TT service provider. The involvement of a professional token generator may be important if an increased level of trust in the quality of the token on the part of the purchaser is important.

Even in the case of industrial companies which use tokens to optimise process or transportation chains do not a priori need to specially regulate participants and this collaboration can be directly and contractually regulated. These applications are not different from those without TT systems.

The criterion of “professional capacity” is therefore suitable for making a distinction between services that should be regulated and private applications. The self-issuance of tokens is an exception. For various reasons, a company may itself



issue tokens, whether for financing purposes, to issue vouchers, to tokenise ownership rights or rights of use to own products, or many other examples. As self-issuance is not a professional TT service, it is not generally subject to the obligation of registration. However, there are cases nevertheless that must be regulated in the government's opinion, in particular in the event that a company self-finances through issuing tokens that are not structured as securities according to the definitions of financial market laws. Taking into account the previous WPPG, that a threshold for the prospectus obligation is defined at five million Francs, the self-issuance of tokens therefore requires registration from a threshold of five million Francs in the TVTG. This registration obligation exists in addition to an existing trading authorisation or other authorisation. As a result, these companies will also be subject to due diligence. Companies that execute self-issuance below this threshold shall also be subject to due diligence for transactions over 1,000 Francs.

In order to register in the TT service provider register, TT service providers must meet the following requirements:

1) Legal capacity:

Those of age who are able to make sound judgements shall have legal capacity (article 11 PGR).

2) Trustworthiness:

A natural person is excluded from rendering a TT Service if:

- they have not been convicted by a court of law for fraudulent bankruptcy, damage to third party creditors, preferring of a creditor with fraudulent intent or grossly negligent interference with creditor's interests (sections

156 to 159 of the Liechtenstein Criminal Code), or have been sentenced to up to three months' imprisonment or a fine of more than 180 daily rates and the conviction has not been expunged; and

- they have not been convicted in the ten years prior to their application due to severe or repeated violations of the provisions of the Law on Unfair Competition, the Consumer Protection Act or a law pursuant to article 5(1) of the Financial Market Supervision Act;
- they have been subject to a futile seizure in the five years prior to application;
- bankruptcy proceedings were brought against them in the five years prior to application or an application to bring bankruptcy proceedings was rejected due insufficient assets to cover the cost pursuant to article 10(3) of the Liechtenstein Bankruptcy Rules (*Konkursordnung* - KO);
- there is another reason which creates serious doubt concerning their reliability.

For legal persons, the requirements must be met by members of their bodies and shareholders, partners or holders who hold a qualified investment of 10% or more in a legal person.

### 3) Professional qualifications:

Those who are sufficiently qualified due to their education or prior career for the task in question shall be considered to be professionally qualified.

Due to the extensive range of applications of the token economy, the number of required qualification is also subject to a large number of differences. TT service providers are expected to specialise in certain fields of application, such as tokenising rights to physical items, licensing rights or book-entry securities. Profes-

sional qualification requirements are not only connected with the specialist area of the application, but also with the degree of complexity of the service. A trading platform which processes a high volume of transactions requires different and more specific expertise in managing risks such as market abuse or money laundering than a token generator which tokenises drinks vouchers. A degree of discretion is required when assessing professional qualifications in order to be able to cover the variety of possible applications. At present there is not any dedicated educational route for many of the applications on which the supervisory authorities can rely when making an assessment. If services relating to the financial market are rendering, the assessment of professional suitability should be heavily based on professional experience in a similar area in the financial market. In order to effectively combat money laundering, financing terrorism and proliferation and to comply with the law on the enforcement of international sanctions, ISG, verifying professional qualifications is also key. Supervisory authorities must also assess which education and professional background is suitable to be sufficiently qualified in this instance.

#### 4) Minimum capital:

The existence of the statutory minimum capital or a guarantee of equal value shall be verified upon registration.

#### 5) Adequate organisational structure:

A TT service provider must prove that its organisational structure is adequate for its intended service, that its areas of responsibility have been clearly defined and that it has a procedure to deal with possible conflicts of interest in place. The supervisory authority must limit itself to examining the completeness of the

submitted documents and checking their contents for plausibility. There is no technical examination of details.

#### 6) Drafting internal procedures and control mechanisms:

A TT service provider must describe its internal procedures and control mechanisms to the supervisory authorities for successful registration. They must be adequate with regard to the nature, scope, complexity and risks of the planned TT services. A plausibility check of the submitted documents may prevent a TT service provider with clear deficiencies operating in Liechtenstein. The supervisory authority must limit itself to examining the completeness of the submitted documents and checking their contents for plausibility. No technical or supervisory examination of the details takes place.

#### 7) Special internal control mechanisms per TT service:

Article 17 stipulates special internal control mechanisms for certain TT service providers. These requirements are principle-based with regard to technology-neutral legislation. The TT is responsible for the correct implementation of the procedures and control mechanisms. These internal control mechanisms must be presented to the supervisory authorities for registration. They will check the completeness and plausibility of the documents and can prevent TT service provider requiring registration with obvious deficiencies operating in Liechtenstein. The examination by the supervisory authorities is also limited here, as is the case with internal procedures and control mechanisms, to completeness and rough plausibility.

In comparison to trading authorisation, the requirements for registering as a TT service provider are higher, in particular the requirements of the trustworthiness

of the qualified parties involved, minimum capital and the internal organisation, procedures and control mechanisms.

The government is certain that these higher requirements are important for legal certainty when dealing with TT service providers, protecting customers, effectively combating money laundering and financing terrorism, complying with the law on the enforcement of international sanctions, ISG, and the reputation of the country.

At the same time, the government is certain that with the newly defined roles, the associated requirements and the supervisory process, TT service providers will be subject to clear rules, thereby creating the required legal certainty which is essential for any economic activity.

TT service providers undertake to always comply with legal requirements and to report all changes to the registration requirements to the supervisory authorities directly. In addition, the government is introducing a reporting obligation to the supervisory authorities for information relevant to supervision.

TT service providers are subject to SPG supervision by the FMA just like other entities subject to due diligence (e.g. financial service providers). Supervisory authorities are also authorised not to allow or deny registration if legal requirements are no longer being met. To do so, it is authorised to demand the documents and information from TT service providers that are required to comply with this Law in addition to ordering and carrying out extraordinary audits, conducting on-site inspections, ordering measures to bring about the lawful state, up to the temporary prohibition of the exercising of the TT service. They may also employ an observer. If it is suspected that a company is rendering TT services without authorisation, the supervisory authorities shall be authorised, without restriction, to demand information and documents.

The government will continue to monitor developments in this area, and will make adjustments to the registration and supervision model if required.

Although it is clear that not all TT service providers in all constellations are subject to financial market laws, the government believes that the financial market supervisory authorities are the most suitable competent supervisory authorities. The regulatory laboratory/financial innovation group and the specialist areas of the FMA have a raft of experience with TT systems and applications. Even now, the FMA already has to examine most of the TT services for demarcation from the financial market laws. For reasons of synergy, the government therefore intends to entrust the FMA with this new task.

### **3.4 Due diligence obligations**

The due diligence obligations to combat money laundering, organised crime and the financing of terrorism are laid down in the Liechtenstein Due Diligence Act (*Sorgfaltspflichtgesetz*). FinTech developments in recent years, in particular virtual currencies or payment tokens, have led to new questions, that can in part be found in the 4th Money Laundering Directive. The government has already implemented these requirements. Since 1 September 2017, pursuant to article 3(1)(f) SPG, exchange bureaus fall within the area of application of the SPG if it exchanges virtual currencies (payment tokens) for legal tender and vice versa in the amount of 1,000 Francs and more. According to article 2(1)(I) SPG, virtual currencies are digital monetary units which can be exchanged for legal tender, or used to purchase goods or services, or to store value, and to thus assume the function of legal tender.

#### International regulatory approaches

European and international committees on the regulation of combating money laundering are observing the development in the environment of virtual curren-

cies very closely and see certain risks that they will face with the adjustments listed below. It is expected that standards will continue to develop in future and consider new findings.

With the 5th Money Laundering Directive (applicable in EU member states from 10 January 2020), new service providers that exchange virtual currencies for legal tender and vice versa and suppliers of electronic wallets will be subject to obligations of due diligence. Exchanging a virtual currency into another virtual currency (payment tokens into payment tokens) is not currently subject to the Money Laundering Directive at European level. Virtual currencies are defined as: *“a digital representation of a value that was not issued or guaranteed by any central bank or public body that is not inevitably pegged to a legally established currency and that does not have the legal status of a currency or money, but that is accepted by natural or legal persons as means of exchange which can be transferred, saved and traded electronically”*.

A supplier of electronic wallets is defined as “suppliers who offer services to secure private, cryptographic keys on behalf of its customers in order to hold, save and transfer virtual currencies”. The 5th Money Laundering Directive further provides for an authorisation requirement or registration requirement (article 47(1)).

The Financial Action Task Force (FATF) amended Recommendation no. 15 in October 2018 that deals with handling new technologies with the following passage:

*“To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and*

*ensuring compliance with the relevant measures called for in the FATF Recommendations”,*

*associated with a definition of “virtual assets” and “virtual asset service providers”:*

*“Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

- i. exchange between virtual assets and fiat currencies;*
- ii. exchange between one or more forms of virtual assets;*
- iii. transfer of virtual assets;*
- iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and*
- v. participation in and provision of financial services related to an issuer’s offer and/or sale of a virtual asset.”*

A virtual asset is defined as:

*„A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.”*

It is clear that the EU and FATF definition aims to only record tokens whose physical counterpart is not yet regulated first of all, and second of all that are similar to means of payment as they are accepted as a means of exchange and therefore as consideration for goods or services.



It must be borne in mind that the FATF guidance (Draft Interpretive Note to FATF Recommendation 15 of 22 February 2019) is at present only in draft form. Any amendments must be considered within the context of the implementation of the 5th Money Laundering Directive. It must be assumed that the exchange of virtual currencies into another virtual currency (payment tokens to payment tokens) will also be subject to money laundering provisions.

It is also undisputed that virtual currencies or payment tokens constitute money pursuant to the compulsory measures imposed based on the law on the enforcement of international sanctions (ISG).

#### Obligations of due diligence in the TVTG

There is the fundamental question as to how the combating of money laundering can be implemented most effectively within the framework of TT systems. Because the recording of existing rights in tokens does not create a new right, and the existing rights are simply subjected to the transmission and legitimization order of TT systems, one could in principle assume that the existing SPG rules would also suffice for TT systems in consideration of the new FATF requirements and the 5th Money Laundering Directive.

However, the government is aware that the benefits of a token economy, in particular the embodiment of rights to assets, and the efficient transfer of these rights, will definitely also open up new possible ways of money laundering, which were not possible in this form until now. Therefore, in order to effectively combat money laundering, it is important to specify appropriate solutions for TT systems. The government's proposal deliberately goes beyond the current international and European standards. In many variants, blockchain technology also certainly offers advantages in detecting and prosecuting money laundering as the transaction chain is saved in a way that cannot be changed and is also publicly

available in many cases. However, we must also be aware that that is not the case for all forms of the technology.

In order to meet international requirements in this area, the government has also opted for a registration system. This ensures the supervision of compliance with the obligations of due diligence and the trustworthiness of individual market participants. Constant, careful supervision is not currently required either by the FATF Recommendations or the 5th Money Laundering Directive. International standards will however certainly evolve.

#### Change and exchange services

Change services relate to money or payment tokens whilst exchange services relate to other tokens. Whilst the changing of legal tender into payment tokens such as Bitcoin and between payment tokens mainly takes place today and shapes the regulatory discussion, a considerably larger variety of exchange services are conceivable in a token economy in which tokens are involved. This complicates the discussion significantly. For this reason, firstly different variants should be described in order to subsequently explain the application of the regulation.

One of the key questions here is the processing of tokens which are primarily used for payment purposes (payment tokens). As explained at the beginning, TT systems allow private individuals to directly hold tokens and transfer them to third parties without requiring a financial intermediary. A token with a monetary or payment function must therefore be compared more with cash than with bank book money, the transfer of which always involves the supervised intermediary. Direct cash payments between private individuals are not subject to the law on due diligence as they are not subject to due diligence.

Even if payment tokens were previously only issued by private individuals, it is fully conceivable that a state in future will issue payment tokens itself (“legal currencies as tokens”). In this case, exchange bureaux will fulfil the key interface function of changing legal currencies – either in the form of book money in a bank account or in the form of physical cash – into the digital money. This activity is then functionally the equivalent of issuing cash at the bank counter or cash machine. This activity is feasible within a currency (e.g. Francs to Francs) or between different currencies (e.g. Francs as book money to digital Euros as cash).

The change of legal currencies into payment tokens essentially therefore follows the same logic. The transfer of book money into payment tokens must therefore also be subject to the same rules as the transfer from book money into cash.

The purely digital exchange between various payment tokens (e.g. in all combinations of tokenised legal currencies and private FIAT payment tokens) is also one of the standard services of the token economy. At present, exchanges between private payment tokens on “crypto-exchanges” are offered in particular.

The “remaining tokens” category is complex: Exchanging a payment token for a general token, such as a token which represents the ownership right to a bicycle, is equivalent to a normal purchase transaction as occurs many times a day in the analogue world (e.g. in bicycle shops), but is not essentially subject to obligations of due diligence. An internet platform to sell goods (e.g. books) can use tokens to process transactions with greater legal certainty. Platforms to exchange goods between private individuals (such as eBay) may also exchange tokens. Fundamentally speaking, the government assumes the same treatment of activities in analogue and digital form.

General information on change and exchange platforms

Change and exchange platforms may be operated in the form of private trade. In such cases, the service provider already has its own tokens that it would like to exchange or buys them in its own name on its own behalf from other traders (see Figure 18). The service provider therefore at no point in time disposes over (payment) tokens that belong to a customer. The figure shows that the service provider disposes over several tokens with its own TT identifier (step 1) and exchanges them for another token which the customer disposes over (step 2). This scenario describes the activity of a TT exchange service provider.

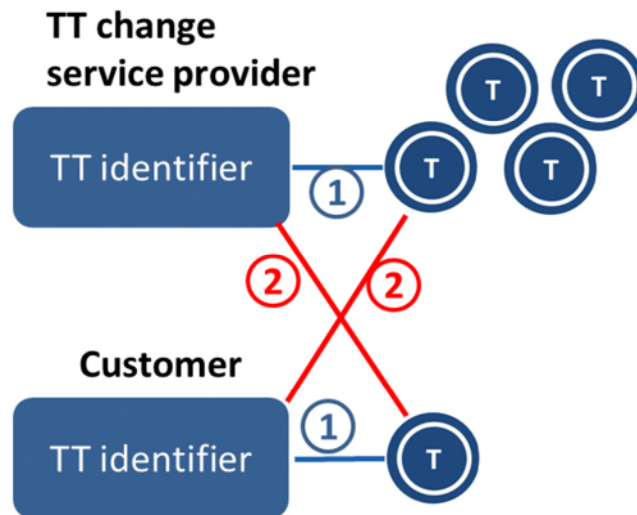
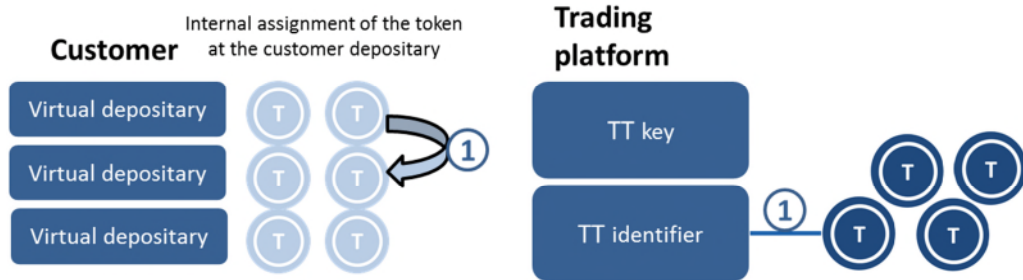


Figure 18: TT exchange service provider with its own trade book

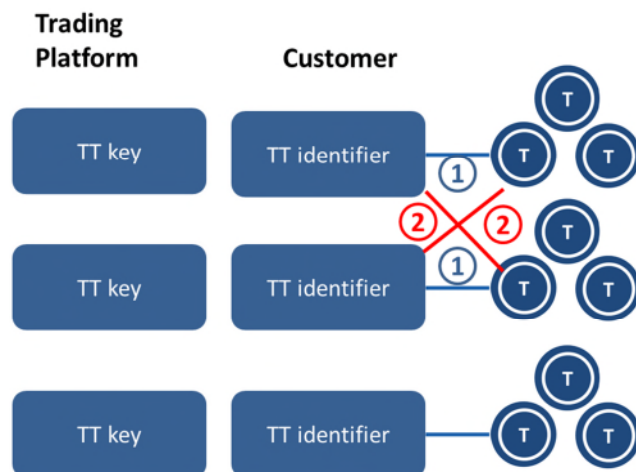
Another form of change and exchange platforms only act as an intermediary between the purchaser and seller without itself appearing as a counterparty to the exchange. Many forms are also possible here: they differ according to the way in which tokens are exchanged: there are platforms which store tokens for customers and assign the tokens to customers in internal accounting. Customers transferring tokens between themselves on the platform is only booked internally. In doing so, the platform must ensure that it has a sufficient number of tokens. Figure 19 illustrates this model and shows that a purchase between two customers of the service provider only takes place virtually through internal rebooking and

that there need not be any real change in the service provider's token depot. This form is normally referred to as a “central trading platform”.



**Figure 19: Exchange platform storing tokens for customers**

A platform can also store TT keys (e.g. private keys) for its customers. In doing so, customer have their own TT identifiers (e.g. public keys) to which their tokens are assigned and which allows TT keys to be stored by the platform in order to execute transactions more easily. Figure 20 illustrates this model and shows the transfer of tokens between customers' TT identifiers (steps 1 and 2).



**Figure 20: Exchange platform with storage of TT keys**

Finally, there are also platforms where customers both have their own TT identifier and a TT key and technically carry out transactions themselves (see figure 21). This form is also referred to as a “decentralised trading platform” without the platform being able to intervene.

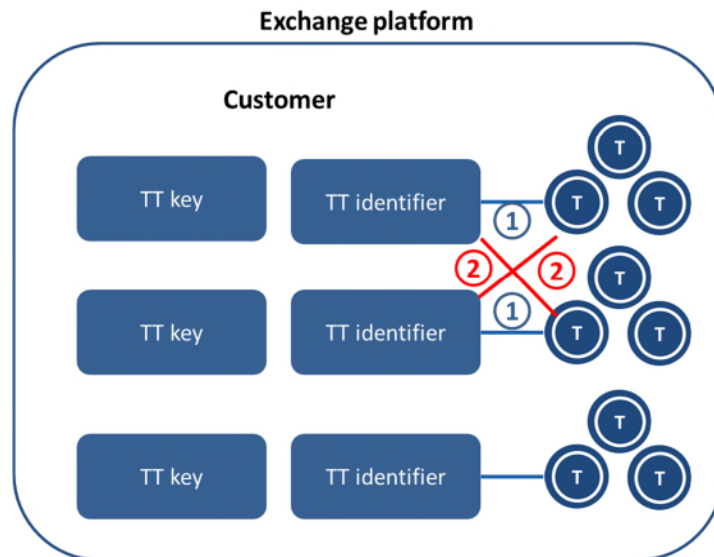


Figure 21: Decentralised trading platform without ability to intervene

### Change service providers

Change in the area of payment tokens and legal currencies can take place by using a physical change machine, by using an online exchange bureau or at a counter (for example at post offices in Liechtenstein). If a change of legal tender with “virtual currencies” takes place, the SPG can already be applied at present. There is a threshold of 1,000 Francs for physical change machines and counter change services. This is compliant with the most recent FATF requirements in this area of occasional transactions that stipulate a maximum threshold of USD/EUR 1,000. In order to fully meet FATF requirements, the change between virtual currencies is now also to be subject to obligations of due diligence.

The Institute of TT exchange service providers (*Institut des VT-Wechseldienstleisters*) includes all service providers who change virtual currencies or payment tokens for other virtual currencies or payment tokens within their own books and hold neither tokens nor TT keys for customers. As money

can be transferred into and out of TT systems via the TT exchange service provider, being subject to the SPG is of particular importance.

The definition of virtual currencies or payment tokens are highly important for the business activity of TT exchange service providers as it determines whether SPG regulations will apply. At present, the existing definition in the SPG is based on the international definition but does not consider that, for example, rights to property or license rights can also be tokenised and that these tokens then have no function as means of payment. The sale of a tokenised good would rather be assigned to the trader with goods who is also subject to due diligence.

For this reason, the government believes it to be important to clarify that this change service only concerns tokens which assume payment functions (payment tokens), regardless of who issues them or how they are designed. Accordingly, an independent definition of payment tokens has been introduced into the TVTG. Both the term payment token and the internationally more common definition of “virtual currency” have been introduced in parallel into the SPG.

### Crypto-exchanges

The government fundamentally believes that there is an increased risk of “crypto-exchanges”, on which payment tokens can be traded, being misused for money laundering. This is in particular the case if the platform holds tokens for customers and the publicly viewable transaction chain is broken, meaning that later it can no longer be understood which address possessed a token at which time. The business model of such a “central crypto-exchange” is fully covered with the role of the TT token depositary.

In contrast, if a “crypto-exchange” stores TT keys for their customers, the risk of money laundering must, in principle, be classified as lower. In this instance, the transaction chain remains intact as every TT identifier can be assigned to a spe-

cific customer. This form of crypto-exchange must register as a “TT key depositary” according to the TVTG.

By subjecting both of these TT service providers to the SPG, the government first of all bears inherent the money laundering risk and implements the relevant FATF regulations.

Likewise, Liechtenstein regulations are also consistent with Swiss regulations in this area, i.e. that trading platforms for virtual currencies which have access to the virtual currencies of their customers are subject to the Money Laundering Act.

In Switzerland, trading platforms for virtual currencies which do not have any access to the tokens of TT keys of their customers, but that can affect customers’ trading platforms, are also subject to money laundering legislation. Purely decentralised trading platforms without such an ability to intervene on the part of the operator must be viewed as equivalent to transactions between private individuals and are not subject to money laundering laws.

The government shares Switzerland’s attitude and clearly stipulates in the SPG that decentralised trading platforms for payment tokens which are able to intervene in customer transactions will also be subject to the SPG.

To date, various activities concerning the change and exchange of payment tokens and legal currencies have been discussed as they naturally come close to “traditional” subject of money laundering.

Exchange platforms which exchanges tokens not qualified as payment tokens must also be discussed per application case in this context.

If, for example, securities tokens are traded, it must be clarified whether a service provider requires authorisation to operate an organised trading facility



(OTF), a multilateral trading facility (MTF) or a regulated market (stock exchange). In these three cases, being subject to the SPG through being required as a bank or securities company to be authorised to operate such a trading platform has already been clarified. If a securities token exchange platform is designed in such a way that it does not require a licence pursuant to the Banking Act, subjecting it to the SPG in a similar way to payment tokens is not appropriate. In this instance, the roles of “TT token depositary” and “TT key depositary” cover the relevant cases. On the other hand, subject the private exchange of securities tokens to the SPG would not be judicially appropriate as certain forms of securities can also be exchanged between private individuals at present without giving rise to the obligations under the SPG.

A further field of application for exchange and trading platforms are tokens that represent rights to physical objects. The spectrum here is enormous: for example, ownership rights to physical assets such as bars of gold or diamonds can be transferred via exchange platforms. In legal terms, how the platform is designed is also important here: if the token is structured as a financial instrument, then the same rules shall apply as for securities tokens. However, there is also the possibility of recording ownership rights digitally in such a way that they do not qualify as financial instruments (similarly to the physical transfer of an object). The government believes that forms of token trading platforms have significantly increased risks with regard to money laundering. As a result, it is appropriate that they be subject to the SPG. These platforms are also fully covered by the roles of “TT token depositary” and “TT key depositary”.

### Token issuance

Token Issuance means the public sale of tokens. Although the general discussion above all concerns the issue of various types of payment tokens, tokens with

rights of use to a software program or investment rights in a company, token issuance may be considerably more versatile in a token economy. Whilst token issuance will continue to play a large role for all kinds of tokenised assets (investments in companies, ownership of assets), tokens with smaller values will also be issued and exchanged in future.

FATF Recommendation No. 15 describes a virtual asset provider as a person who participates in an issuance or provides financial services as an agent. The government therefore intends to subject token Issuers that operate professionally on behalf of others to the obligation of registration and therefore obligations of due diligence. In doing so, international regulations have been met. This should also apply for all types of token.

However, the government also sees a certain risk of money laundering or financing terrorism for own-issues, which is why obligations of due diligence should be applied for own-issues starting from certain thresholds. Own-issues are essentially not covered by FATF Recommendation No. 15. Nevertheless, the government decided to also subject own-issues to obligations of due diligence with certain restrictions. First of all, own-issues from five million Francs and over are also required to register and be subject to due diligence. Secondly, obligations of due diligence shall also apply starting from transactions of 1,000 Francs for own-issues that do not require registration (under five million Francs). The thresholds have been taken from the Securities Prospectus Act where European legislation also provided for a regulation requirement starting from five million Francs. The government is aware that international recommendations and requirements have been exceeded with the regulation of own-issues. However, it views this as necessary in order to protect Liechtenstein's financial centre from money laundering and financing terrorism.

### Tokenising rights to physical items

The tokenisation of rights to physical items can also be very varied. The government consciously does not prescribe the use of a physical validator as there are many application possibilities where this could lead to disproportionately high complexity. The role of a physical validator is therefore in particular sought after for high-value assets where the legal certainty between the digital and analogue world is vital. As high-value assets can be introduced onto TT systems when tokenising rights to items, the role of the physical validator in combating money laundering must be emphasised. For this reason, the government intends to subject this activity to obligations of due diligence.

### Storing tokens and TT keys

Service providers storing tokens play a central role in the token economy. Storage is not only relevant in crypto-exchanges, but can be useful in many other services.

As addresses (TT identifiers) are separated from the owner when storing tokens, there is a particular risk of money laundering. For this reason, the government proposes classifying TT token depositories as being entities subject to due diligence. Being subject to the SPG depends on the type of rights represented in the token.

Storing TT keys is not only used for crypto-exchanges but also for certain kinds of wallet providers and many other applications. Even if a TT Depository only keeps TT keys and so there are no special risks from a money laundering perspective, it is still a possible gateway for tokens to enter into Liechtenstein. Subjection to the SPG is intended to help clarify the origin of assets held in Liechtenstein.

Application of obligations of due diligence for foreign subsidiaries

The global application of the due diligence standard according to article 16 SPG also applies for TT service providers subject to due diligence.

### 3.5 Book-entry securities

#### Overview

Since the original version of the PGR in 1926, Liechtenstein securities law, regardless of the possibility of issuing uncertificated securities, has been relatively strongly influenced by the notion of the connection of a right with a physical information carrier (certificate) (see section 73(1) Final Part PGR). Due to the fact that the Liechtenstein legal system has immobilised and dematerialised securities, i.e. book-entry securities, there has been no reason to adopt the Swiss Book-Entry Securities Act. Promissory note law is a significant manifestation of dematerialised securities where the step towards dematerialisation took place with the transition to registered promissory notes (Law of 31 August 2016 on the change of property law, Liechtenstein Law Gazette No. 349).

The obligation to securitise a right in a physical document has long been outdated and is proving more than ever to be an obstacle to digitalising the economy. With section 81a, Final Part PGR, the government is therefore proposing the positive creation of a genuine book-entry security with all the functions of a security of public faith (bearer or order paper). A security has public faith as a bearer or order paper; this is due to its double protection of the legitimate expectations of an acquirer: Firstly, the legitimate expectations in the seller's power of disposal are protected; secondly, the legitimate expectations in the securitised right are protected.

The basis of a genuine book-entry security is an electronic register in which both the issue and the transfer of book-entry securities must be recorded. At the same time, section 81a, Final Part PGR creates a new interface between the TVTG and securities law. This is because the value right register can also be kept on the basis of a TT system; such systems are particularly suitable for this pur-

pose because they enable a clear and seamless assignment of legal title to each book-entry security and cannot be manipulated. Consequently, the issuing of securities and the clearing and settlement of securities transactions on TT Systems are considered to be one of the key potential applications for TT technologies.

In the consultation process, the need to introduce a real book-entry security was in part discussed. It is true that digital value chains have been created despite the necessity of a physical information carrier. However, more or less complex and artificial substitute constructions were necessary to do this, e.g. by issuing global certificates which had to be deposited with a depositary. However, securities certificates have long since lost their original significance, which is why it is only logical to abolish them altogether and replace them with a register-supported information carrier. Moreover, it should be noted that the legal concept of the book-entry security is not new to Liechtenstein law. In addition to the aforementioned registered promissory notes, which have functions under securities law based on the entry in the register, the Liechtenstein Constitutional Court in 1975, in an obiter dictum, recorded the possibility that founder's rights in an establishment may be structured as "uncertificated book-entry securities" (Liechtenstein Constitutional Court 1975/002, ELG 1973, 381, 383). Since its original version of 1926, the PGR has also required the possibility of issuing membership shares to legal persons as a book-entry security (article 149(3) PGR). However, the transfer or pledging of such book-entry securities takes place according to principles of assignment law, meaning that it is not possible to acquire them in good faith. A real system of book-entry securities should therefore be introduced into the Liechtenstein legal system in a legally positive manner.

Finally, the explicit legalisation of the legal concept of book-entry securities is also in line with its development abroad. In particular, the introduction of a real

book-entry security will also be a key element of the legal framework for the token economy in Switzerland (see the preliminary draft of a federal law on the adjustment of the federal law to developments in the technology of distributed electronic registers of 22 March 2019). In Germany, the introduction of electronic securities is also being discussed in a key issues paper of the Ministry of Finance and the Ministry of Justice, but is currently limited to debt securities (Ministry of Finance/Ministry of Justice, key issues for the regulatory treatment of electronic securities and crypto-tokens, Berlin, 8 March 2019).

### **The term “book-entry security”**

According to the legal definition in section 81a(1), Final Part of the PGR, book-entry securities are “rights with the same function as securities”. They are not therefore securitised rights that have been structured in such a way that they meet the same functions as a security of public faith. These generally have the following functions: the simple transfer of the right by transfer of the (possibly endorsed) document (transport function); the legitimation of the contact person through ownership of the certificate (legitimation function) or the release of the debtor upon payment to the (possibly endorsed) holder of the certificate (liberation function); the acquisition by virtue of good faith of the right in accordance with the principles of property law (transaction protection function); the restriction of objections to those which are directed against the validity of the certificate or which result from the certificate (objection restriction).

In the case of traditional securities, all these functions are based on the securitisation of the right in certificate or the ownership of this certificate. In the case of a book-entry security, the representation of the right is waived; a register takes the place of the certificate. Book-entry rights therefore arise through entry in the register and are transferred or pledged through entry in the register and can also

be acquired by the person entered in the register as the legal owner by virtue of good faith. Both the transport function, the legitimisation function, the liberation function, the transaction protection function and the objection restriction are, in other words, based on the entry in the register. A real book-entry security therefore has all the functions of a security (function equivalence).

This functional equivalence justifies the unrestricted equation of book-entry securities with securities pursuant to section 81a, Final Part of the new PGR. Whenever Liechtenstein law concerns securities, this will in future also include book-entry securities, unless differentiation is necessary due to differences in the information carrier. In the opinion of the government, therefore, a comprehensive adaptation of the relevant laws is no longer necessary.

Section 81a, Final Part PGR does not say anything about which rights can be recorded in the form of book-entry securities. In practice, the focus will be both on fungible claims and membership positions in corporations and companies. In principle, however, it must be possible to securitise all kinds of subjective rights that can be the subject of legal transactions. However, there is no reason at all for a more precise or restrictive description, since it also applies to physical securities that these can generally have "rights" as their subject (see section 73(1), Final Part PGR).

### **Requirements for the issue of book-entry securities (section 81a(1), Final Part of the new PGR)**

Section 81a(1), Final Part of the new PGR first of all redefines book-entry securities as "rights with the same function as securities". As a condition for issuing book-entry securities, it also requires that authorisation to do so come from the issue conditions (in the case of debt securities and similar) or the company's arti-



cles of association (in the case of membership rights) or that the entities entitled to do so having granted their approval. Whilst the option of securitising rights has existing for centuries, the legal concept of a book-entry security is still relatively new, which is why investors, shareholders and other entitled parties must be specially informed of this concept.

### **Book-entry security register (section 81a(2), Final Part of the new PGR)**

In the case of book-entry securities, information carriers are not physical certificates, but a book-entry securities register. For this reason, section 81a(2) of the new PGR obliges debtors to manage a register on the book-entry securities they issued in which the number and denomination of the issued book-entry securities and the holder of the book-entry securities are to be recorded. All securities functions that correspond to book-entry securities are based on entries in this register. Book-entry securities arise with the entry into the register (section 81a(3) of the new PGR) and are transferred or pledged by entry in the register (section 81a(4) of the new PGR). The acquisition in good faith of book-entry securities refers to this entry (section 81a(5) of the new PGR) as does the legitimisation and liberation function (section 81a(6) of the new PGR).

The book-entry securities register does not however need to be managed based on TT systems. Another requirement is essential, which section 81a(2)(3) of the new PGR names: book-entry securities registers must be organised in such a way that they prevent the unauthorised intervention of the debtor in the rights of creditors. Whilst physical securities are no longer in the hands of the debtor after issuance and the debtor no longer has any influence over them, the book-entry securities register is managed by the debtor. It is therefore conceivable that the debtor would interfere without authorisation with the legal title or even the existence of the book-entry rights. The debtor therefore has considerable options

for misuse and, as a result, can make it more difficult for creditors to exercise or transfer their rights, or prevent them from doing so.

The law therefore requires the debtor to organise their book-entry securities register in such a way that such unauthorised interference is not possible. This is readily possible with TT systems by granting creditors participation or control rights. However, the new requirement pursuant to section 81a(2)(3) of the new PGR can also be met by outsourcing the maintenance of the book-entry securities register to an independent third party; in this case, the book-entry securities register does not necessarily have to be maintained on the basis of a TT system. A register that does not meet these requirements is not a book-entry securities register within the meaning of the law, which is why rights entered in it do not qualify as book-entry securities.

#### **Emergence of book-entry securities (section 81a(3), Final Part of the new PGR)**

Pursuant to section 81a(3), Final Part PGR, book-entry securities are newly created upon entry in the book-entry securities register and continue to exist only in accordance with said entry". Entry into the book-entry register therefore has a constitutive effect. A legal consequence of being entered in the register is that the right represented in the book-entry security will be subject to the transfer and legitimisation order pursuant to section 81(a)(4-6), Final Part of the new PGR.

#### **Transferring and pledging book-entry securities (section 81a(4), Final Part of the new PGR)**

Legal title to book-entry securities or the order of restricted in rem rights to book-entry securities are transferred by entering the acquirer or the entitled party, restricted in rem, in the book-entry securities register (section 81a(4), Final

Part of the new PGR). Entry also has a constitutive effect in this instance. Section 81a(4), Final Part of the new PGR only deals with the act of transfer as customary in the law on moveables, and does not deal with the further requirements according to the general principles of asset law (legal basis, power of disposal).

Book-entry securities can also be encumbered with restricted in rem rights according to the explicit working of section 81a(4), Final Part of the new PGR, where, in practice, right of lien and rights of usufruct are the focus. As book-entry securities are registered securities, there is also the option of non-proprietary right of lien, meaning that both the holder and the pledgee are listed in the register. Although this represents a breach of the principle of pledged collateral (article 365(1) and (3) Property Law), it can be well justified. There is no need for adjustment in terms of property law as article 365(1) already reserves statutory exceptions; section 81a (4), Final Part of the new PGR is such an exception. All further questions in connection with the pledging of book-entry securities can easily be solved by applying article 365 et seq. of the Property Law *mutatis mutandis*.

Book-entry securities can only be transferred or pledged by entry in the register; a transfer or pledge according to principles of claims law is also not possible. In general securities law, the possibility of a parallel disposal is generally permitted both according to principles of securities law and claims law. However, the assignee cannot assert claims securitised in a bearer paper as long as they do not hold the paper in their hands; until then, the debtor can only make payment to the holder of the certificate with discharging effect. As a result, the holder of the certificate shall prevail in the assignment of claims securitised by securities law. The same applies for book-entry securities: In the case of assigning or pledging of book-entry right due to the legitimation and liberation function of the book-entry security (section 81a(6), Final Part of the new PGR), the holder registered in

the book-entry securities register shall always prevail as a result as the debtor can and must pay the holder. In view of this situation, the possibility of also disposing over book-entry securities by means of assignment does not appear particularly logical; it can therefore be excluded without any further consideration.

Finally, there is also a need for clarification with regard to order papers issued in the form of book-entry securities. Physical order papers are transferred through tradition and endorsement. Endorsement is not possible for book-entry securities. For this reason, section 81a(4)(2), Final Part of the new PGR now clarifies that the entry in the register has all the legal effects of an endorsement in the case of order papers.

#### **Transaction protection function (section 81a(5), Final Part of the new PGR)**

Unlike non-securitised claims, a good-faith purchase of securities is possible, being based on possession of the certificate (including a formally uninterrupted endorsement chain, as applicable). In the case of book-entry securities, entry in the book-entry securities register takes the place of the possession of a certificate. A purchaser who acquires the book-entry security from the holder entered into the register in good faith is to be protected when making this purchase, even if the holder was not authorised to dispose of the security under substantive law.

#### **Liberation and legitimisation function (section 81a(6), Final Part of the new PGR)**

Section 81a(6), Final Part of the new PGR governs the liberation and legitimisation function of book-entry securities. The legitimisation function means that the debtor is entitled and obliged to pay the holder registered in the book-entry securities register. No further proof of legitimisation may be required. As a result, the

debtor is released by paying the registered holder unless they knew or should have known upon the exercise of due diligence that the holder is not the materially entitled party.

### **Book-entry securities on legal conditions under company law**

Shares, share-like instruments (participation and “jouissance” rights) and other membership rights under company law that may be securitised as securities (article 149(f) PGR) can be issued as book-entry securities. If legal positions under company law are issued as securities or book-entry securities, regulations under company law must also be complied with in addition to regulations under securities law when they are transferred. Generally, a full acquisition of a legal position under company law requires that both requirements under securities law and under company law be fully met. It must also be noted that the content of securities or book-entry securities that securitises legal positions under company law is not exclusively determined according to the security, but primarily according to the articles of association and company resolutions. The legitimisation and liberation function of securities or book-entry securities under company law only comes into effect *mutatis mutandis*, as is also the case for the objection restriction.

The following structures are limited to shares as in practice only they are issued as securities.

### **Bearer shares**

Pursuant to article 323(4) PGR, bearer shares must be transferred in accordance with the regulations of securities law (i.e. by transferring ownership of the share certificate). For non-listed company shares, an obligation to deposit bearer

shares with the depositary was created as a result of the PGR revisions (immobilisation of bearer shares and introduction of a sanction mechanism with regard to the management of the share register for registered shares; Lichtenstein Law Gazette No. 67). Bearer shares must be deposited with a depositary (article 326a(1) PGR) to be appointed by the company (article 326b PGR). The depositary must maintain a register with the information named in article 326c PGR. With regard to the company, a person recorded in the register shall be considered a shareholder (article 326c(2) PGR). Shareholder rights from bearer shares can only be asserted if the share is deposited with the depositary and all information regarding the holder of the bearer shares has been registered (article 326f PGR). A legal situation is created which mainly corresponds to the legal situation in the case of registered shares.

This provision can also be productive for bearer shares that are issued in the form of book-entry securities pursuant to section 81a, Final Part of the new PGR. Instead of a deposit pursuant to article 326a(1) PGR, which is not possible without a physical title, the issue will be registered with the depositary. The book-entry securities created through registration in the book-entry securities register pursuant to section 81a(3), Final Part of the PGR must therefore be registered in a stock account with the depositary. All of the book-entry securities must be registered.

For the transfer of bearer shares, article 325h PGR establishes that shareholders must have informed the depositary of their intention to do so (paragraph 1), where such information must identify the purchaser. Pursuant to article 326h(3) PGR, the “transfer of bearer shares shall become effective once the purchaser has been registered pursuant to article 326c”. Although this regulation leaves open the relationship between them and the acquisition process under securities law, it can be assumed, in exactly the same way as with registered shares (in-

stantly)), that requirements under securities law and company law must be met cumulatively in order for bearer shares to be legally transferred. For bearer shares deposited with a depositary, this means that a transfer of the ownership to the purchaser must take place in addition to entry in the register. Ownership is therefore transferred by means of an instruction to hold the shares from the selling shareholder (as an indirect, independent possessor) to the depositary (as a direct, dependent possessor). The securities law part of the transfer process is concluded when the depositary receives the instruction to hold the shares. In respect of the company, a shareholder is only recognised if they are also entered in the register; i.e. before entry, the purchaser can neither assert shareholders' rights nor receive payments from the company. Although transfers under securities and company law are therefore combined in a single action, they must however be clearly distinguished in legal terms other as they fundamentally differ both in the facts and in the legal consequences.

For bearer shares that are issued in the form of a book-entry security pursuant to section 81a, Final Part of the new PGR, transfers first of all require entry into the company's book-entry securities register (section 81a(4) of the new PGR) and secondly the entry of the purchaser in the depositary's register. In other words, the company must ensure the coordination of the entries in the register and book-entry securities register. Naturally, this can also take place as a result of management of the book-entry securities register for bearer shares being transferred to a depositary pursuant to article 326b PGR.

### **Registered shares**

It also applies to registered shares that the transfer of legal title by way of singular succession has both an aspect under securities law and company law. Registered shares are considered to be order papers (article 327(1) PGR) provided that

the articles of association do not stipulate the transfer by way of assignment (in this case they are real registered shares). From the point of view of securities law, the transfer is effected by endorsement and transfer of ownership of the title (article 327(2) PGR). Endorsement may also be an endorsement in blank; in this case, the transfer only requires the tradition of the title under securities law. From a perspective of company law, the purchaser must also be registered in the share register (article 328 PGR) where “with regard to the company, those who are registered in the share register shall be considered shareholders” (article 328(2)PGR). The entry into the share register must be noted by the company on the share title (article 328(4) PGR). The share register may also be managed electronically; it must be held at the company’s headquarters (article 329a PGR).

Registered shares may also be issued in future in the form of book-entry securities. Section 81s(4), Final Part of the new PGR clarifies in this instance that entry into the book-entry securities register will have all the effects of an endorsement in the case of a transfer of a book-entry security that is considered to be an order paper. Article 328(4) PGR therefore does not apply to registered shares in the form of book-entry securities due to a lack of physical title. The issue of registered shares in the form of book-entry securities does not affect requirements under company law (entry into the share register) where the book-entry securities register and share register can be managed based on the same electronic system.

## **Conclusion**

This proposal for a new section 81a, Final Part PGR makes a positive case for the legal device of a book-entry security into Liechtenstein law and simultaneously creates the interface between securities law and the TVTG. This creates the possibility of issuing book-entry securities in the form of tokens on a decentralised database and transferring them there. TT Systems are perfectly suited for issuing



and transferring book-entry securities because they enable an unambiguous and uninterrupted allocation of the legal title to each uncertificated right and are tamper-proof. Consequently, the issuing of securities and the clearing and settlement of securities transactions on TT Systems are considered to be one of the key potential applications for TT technologies. Section 81a, Final Part PGR is modelled on article 973c of the Swiss Code of Obligations, however, it extends further in various aspects.

### **3.6 Scope of the Law**

With this Law, the Government is seeking to strengthen legal certainty relating to transactions with digital rights on TT Systems. TT Service Providers that provide relevant services for the protection of users must comply with the minimum standards set out in this Law. Consequently, this Law is applicable to all TT Service Providers domiciled in Liechtenstein who commercially provide services subject to registration. However, it is not applicable to TT Service Providers domiciled abroad and who render TT services for persons resident in Liechtenstein. This would mean an inappropriate restriction of the market access to the token economy for persons resident in Liechtenstein. As a result of the TVTG, the government is creating an option for users to elect TT systems when selecting their TT service provider.

The TVTG should be seen as a supplement to the existing special law regulations. If, for example, banking or securities services are offered on a TT system, the provisions of the Banking Act or VVG apply. However, already approved financial intermediaries who would like to render a TT service must register separately with the FMA. Facts where the special laws named in article 5(1) FMAG lay down an exception are also covered by the TVTG (for example, if the issue of a security token does not require a prospect as an exception or if a token that would be qualified as e-money falls under the exceptions according to the EGG (*El-*

*elektronischer Geschäftsverkehr-Gesetz* - Electronic Transaction Law). The TVTG would like to fully regulate professional activities in the area of blockchain applications and cryptocurrencies.

**Unofficial Translation of the Draft Law on Tokens and TT Service  
Providers (Token and TT Service Provider Act)**

**Disclaimer**

English is not an official language of the Principality of Liechtenstein. This translation is provided for information purposes only and has no legal force. This translation has been compiled with the utmost care. However, the Government of Liechtenstein cannot accept any liability for inaccurate translations.

Please note that this Act is only in draft version and currently in the parliamentary process.

## **II. GOVERNMENT BILL**

### **1.1 Law on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG)**

#### **Law**

of ...

#### **on Tokens and TT Service Providers (Token and TT Service Provider Act; TVTG)**

I hereby grant My consent to the following resolution adopted by Parliament:

#### **I. General provisions**

##### **Article 1**

##### *Object and Purpose*

1) This law establishes the legal framework for all transaction systems based on Trustworthy Technology and in particular governs:

- a) The basis in terms of civil law with regard to Tokens and the representation of rights through Tokens and their transfer;
- b) The supervision and rights and obligations of TT Service Providers.

2) It aims:

- a) to ensure trust in digital legal communication; in particular, in the financial and economic sector, and the protection of users in TT Systems;
- b) to create an excellent, innovation-friendly, and technology-neutral framework for rendering services rendered on or concerning TT Systems.

## Article 2

### *Definitions and designations*

1) The following definitions are established for the purposes of this Act:

- a) “Trustworthy Technology (TT)”: Technologies through which the integrity of Tokens, the clear assignment of Tokens to TT Identifiers and the disposal over Tokens is ensured;
- b) “TT Systems”: Transaction systems which allow for the secure transfer and storage of Tokens and the rendering of services based on this by means of trustworthy technology;
- c) “Token”: a piece of information on a TT System which:
  - 1. can represent claims or rights of memberships against a person, rights to property, or other absolute or relative rights; and
  - 2. is assigned to one or more TT Identifiers;
- d) “Payment Tokens”: Tokens that are accepted to fulfill contractual obligations and therefore replace legal tender in this respect;
- e) “TT Identifier”: an identifier that allows for the clear assignment of Tokens;
- f) “TT Keys”: a key that allows for disposal over Tokens;
- g) “Users”: people who dispose of Tokens and/or use the TT Services;
- h) “Token Issuance”: the public offering of Tokens;

- i) “Basic Information”: Information about Tokens to be offered to the public, enabling the user to make a judgement about the rights and risks associated with the Tokens as well as the TT service providers involved;
- k) “TT Service Provider”: a person who exercises one or more functions under (l) to (u);
- l) “Token Issuer”: a person who publicly offers Tokens in their own name or in the name of a client;
- m) “Token Generator”: a person who generates one or more Tokens;
- n) “TT Key Depositary”: a person who safeguards TT Keys for clients;
- o) “TT Token Depositary”: a person who safeguards Tokens in the name of and on account of others;
- p) “Physical Validator”: a person who ensures the enforcement of rights in accordance with the agreement, in terms of property law, represented in Tokens on TT systems;
- q) “TT Protector”: a person who holds Tokens on TT Systems in their own name on account for a third party;
- r) “TT Exchange Service Provider”: a person who exchanges legal tender for Payment Tokens (and vice versa) and Payment Tokens for Payment Tokens;
- s) “TT Verifying Authority”: a person who verifies the legal capacity and the requirements for the disposal over a Token;
- t) “TT Price Service Provider”: a person who provides TT System users with aggregated price information on the basis of purchase and sale offers or completed transactions;

- u) “TT Identity Service Provider”: a person who identifies the person in possession of the right of disposal related to a Token and records it in a directory;

2) The designations used in this Act to denote persons and functions apply equally to the male and female genders.

## **II. Civil basis**

### Article 3

#### *Object and scope*

1) This chapter governs the qualification of Tokens and their disposal on TT Systems under civil law.

2) It applies if:

- a) Tokens are generated or issued by a TT Service Provider with headquarters or place of residence in Liechtenstein; or
- b) Parties declare its provisions to expressly apply in a legal transaction over Tokens.

3) Articles 4 to 6 and 9 also apply correspondingly to Tokens that do not represent any rights.

Article 4

*Qualification of Tokens*

If Liechtenstein Law is applicable according to article 3, the Token is considered to be an asset located in Liechtenstein.

Article 5

*Power of Disposal and Right of Disposal*

1) The TT key holder has the power of disposal over the Token.

2) It is further assumed that the person possessing the power of Token disposal also has the right to dispose of the Token. For every previous holder of the power of disposal, it is presumed that he was the person possessing the right of disposal at the time of his ownership.

3) If someone is the holder of a power of disposal without wanting to be the person possessing the right of disposal, he can rely on the person from whom he received the Token in good faith is the person possessing the right of disposal.

Article 6

*Disposal over Tokens*

1) Disposal is:

- a) the transfer of the right of disposal over the Token; or
- b) the justification of a securities or a right of usufruct to a Token.

2) Disposal over a Token requires that:



- a) the transfer of the Token is concluded in line with the regulations of the TT System where a restricted in rem right to a Token can also be ordered without transfer, if this is apparent to third parties and clearly establishes the time of ordering;
- b) the transferring party and the receiving party unanimously declare to transfer the right of disposal over the Token, or that they want to justify a restricted in rem right;
- c) the transferring party is the person possessing the right of disposal pursuant to article 5; article 9 remains unaffected.

3) If a Token is disposed of without reason or a subsequent reason fails to exist, the revocation shall be accomplished in accordance with the provisions of the Enrichment Law (sections 1431 et seq. ABGB).

## Article 7

### *Effects of Disposal*

1) Disposal over the Token results in the disposal over the right represented by the Token.

2) If the legal effect under (1) does not come into force by law, the person obliged, as a result of the disposal over the Token, must ensure through suitable measures that:

- a) the disposal over a Token directly or indirectly results in the disposal over the represented right, and
- b) a competing disposal over the represented right is excluded.

3) The disposal over a Token is also legally binding in the event of enforcement proceedings against the transferor and effective vis-à-vis third parties, if the transfer:

- a) was activated in the TT system prior to the commencement of the legal proceedings, or
- b) was activated in the TT the system after the initiation of the legal proceedings and was executed on the day of the proceeding's opening, provided that the accepting party proves that he was without knowledge of the proceeding's opening or would have remained without knowledge upon the exercise of due diligence.

#### Article 8

##### *Legitimacy and exemption*

1) The person possessing the right of disposal reported by the TT System is considered the lawful holder of the right represented in the Token in respect of the Obligor.

2) By payment, the Obligor is withdrawn from his obligation against the person who has the power of disposal as reported by the TT system, unless he knew, or should have known with due care, that he is not the lawful owner of the right.

#### Article 9

##### *Acquisition in Good Faith*

Those who receive Tokens in good faith, free of charge, for the purpose of acquiring the right of disposal, or a restricted in rem right, are to be protected in their acquisition, even if the transferring party was not entitled to the disposal

over the Token; unless the recipient party had been aware of the lack of right of disposal, or should have been aware of such upon the exercise of due diligence.

#### Article 10

##### *Cancellation of Tokens*

1) If a TT Key is unaccounted for, or a Token is otherwise not functional, the person who possessed the right of disposal at the time of the loss, or when the Token became non-functional, can apply for the Token to be cancelled in non-contentious proceedings.

2) For this purpose, the applicant must convince the court of his right of disposal and the loss of the TT Key, or the non-functionality of the Token. The District Court is competent in this matter.

3) The respondent is the person obliged due to the right represented in the Token.

4) The applicant may also assert his right without Tokens upon cancellation or demand the generation of a new Token at its own expense.

### **III. Supervision of TT Service Providers**

#### **A. General**

##### Article 11

##### *Object and scope*

1) This chapter governs the registration and supervision of TT Service Providers with headquarters or place of residence in Liechtenstein and their rights and obligations.

2) It does not apply to the country, municipalities or municipal associations or public companies when acting as officials.

#### **B. Registration of TT Service Providers**

##### **1. Obligation and requirements of registration**

##### Article 12

##### *Registration obligation*

1) Persons with headquarters or place of residence in Liechtenstein who wish to professionally act as TT Service Providers must apply to be entered into the TT Service Provider Register in writing (article 23) with the FMA before providing a service for the first time.

2) Token Issuers with headquarters or place of residence in Liechtenstein who issue Tokens in their own name or in the name of a client in a non-professional capacity, must apply to be entered into the TT Service Provider Register in writing with the FMA before beginning an activity involving Tokens amounting to an issuance value of CHF 5 million or more to be issued within a period of twelve months.

## Article 13

*Registration requirements*

1) An entry in the TT Service Provider Register (article 23) requires the applicant to:

- a) be capable of action;
- b) be reliable (article 14);
- c) be technically suitable (article 15);
- d) have their headquarters or place of residence in Liechtenstein;
- e) have the necessary minimum capital (article 16), where appropriate;
- f) have a suitable organisational structure with defined areas of responsibility, including procedures for dealing with conflicts of interest;
- g) have written internal proceedings and control mechanisms that are appropriate in terms of the type, scope, complexity, and risks of the TT Services provided; including ensuring sufficient documentation of these mechanisms;
- e) have special internal control mechanisms (article 17), where appropriate;
- i) have authorisation pursuant to the Trustees Act if he intends to act as a TT Protector;
- k) have relevant special statutory authorisation if he intends to conduct activity that is subject to an additional special statutory authorisation obligation.

2) The government may rewrite the registration requirements in (1) subject to articles 14 to 17 in more detail by issuing an ordinance.

## Article 14

### *Reliability*

1) A natural person is excluded from rendering a TT Service if:

- a) they have been convicted by a court of law for fraudulent bankruptcy, damage to third party creditors, preferring of a creditor with fraudulent intent or grossly negligent interference with creditor's interests (sections 156 to 159 of the Liechtenstein Criminal Code), or have been sentenced to up to three months' imprisonment or a fine of more than 180 daily rates and the conviction has not been expunged; and
- b) they have been convicted, in the ten years prior to their application, of severe or repeated violations of the provisions of the Law on Unfair Competition, the Consumer Protection Act, or a law pursuant to article 5(1) of the Financial Market Supervision Act;
- c) they have been subject to a futile seizure in the five years prior to application;
- d) bankruptcy proceedings were brought against them in the five years prior to application, or an application to bring bankruptcy proceedings was rejected due insufficient assets to cover the cost pursuant to article 10(3) of the Liechtenstein Bankruptcy Rules (*Konkursordnung* - KO);
- e) there is another reason which creates serious doubt concerning their reliability.

2) (1) (a) to (d) also applies for foreign decisions and proceedings if the underlying action constitutes a criminal offence pursuant to Liechtenstein law.

3) For legal persons, the requirements under (1) must be met by members of their bodies and shareholders, partners, or legal persons who hold a qualified investment of 10% or more.

4) Upon request, the FMA may allow for exclusion under (1) and (2) if committing the same or similar offence when rendering the TT Service is not considered to fall within the nature of a criminal offence, and not considered characteristic of the personality of the person sentenced.

#### Article 15

##### *Technical suitability*

Those who are sufficiently technically qualified for the task in question due to their education or prior career shall be considered technically suitable.

#### Article 16

##### *Minimum capital*

1) Applicants who intend to act as TT Service Providers pursuant to article 2(1) (l), (n), (o), (p), and (r) must have the appropriate minimum capital or a guarantee of the same value before starting their activity. Minimum capital is:

- a) for Token Issuers pursuant to article 12(1):
  - 1. 50,000 Francs, if Tokens with a total value of up to and including 5 million Francs are issued within a period of twelve months;
  - 2. 100,000 Francs, if Tokens with a total value of more than 5 million Francs are issued within a period of twelve months;
  - 3. 250,000 Francs, if Tokens with a total value of more than 25 million Francs are issued within a period of twelve months;

- b) for TT Key Depositories: 100,000 Francs;
- c) for TT Token Depositories: 100,000 Francs;
- d) for TT Exchange Service Providers:
  - 1. 30,000 Francs, if transactions with a total value of more than 150,000 Francs up to and including 1 million Francs are issued within a period of twelve months;
  - 2. 100,000 Francs, if transactions with a total value of more than 1 million Francs are issued within a period of twelve months;
- e) for Physical Validators:
  - 1. 125,000 Francs, if the value of the property whose contractual enforcements is guaranteed by the Physical Validator does not exceed 10 million Francs;
  - 2. 250,000 Francs, if the value of the property whose contractual enforcements is guaranteed by the Physical Validator exceeds 10 million Francs.

2) The minimum capital requirements under (1) must be adhered to at all times.

## Article 17

### *Special internal control mechanisms*

1) Applicants who intend to act as TT Service Providers pursuant to article 2(1)(l) to (u) must have suitable internal control mechanisms before starting their activity, ensuring the following:

- a) for Token Issuers:



1. disclosure of basic information (articles 30 to 38) at any time during Token Issuance and for at least ten years afterwards;
  2. the prevention of abuse with regard to the option of Token recipients waiving basic information (article 31(1)(a));
  3. the execution of Token Issuance according to the conditions of the basic information;
  4. the maintenance of the provided services in the event of interruptions during the Token Issuance (business continuity management);
- b) for Token Generators, the use of suitable measures, ensuring that:
1. the right is correctly represented in the Token during the Token's lifetime;
  2. that the disposal over a Token directly results in the disposal over the represented right;
  3. a competing disposal over the represented right is excluded both under the rules of the TT system and the provisions of applicable law.
- c) for TT Key Depositories:
1. establishing suitable security measures; which in particular prevent the loss or abuse of TT Keys;
  2. the separate safekeeping of customers' TT Keys from the business assets of the TT Key Depositary; and
  3. the maintenance of services in the event of interruptions (business continuity management);
- d) for TT Token Depositories:
1. establishing suitable security measures; which, in particular, prevent the loss or abuse of TT Keys;

2. the separate safekeeping of customers' Tokens from the business assets of the TT Token Depositary; and
  3. the clear assignment of customers' Tokens;
  4. the execution of customers' orders in line with agreements;
  5. the maintenance of services in the event of interruptions (business continuity management);
- e) for Physical Validators, their liability in the event that rights to property guaranteed by the Physical Validator cannot be enforced in accordance with the contract;
- f) for TT Protectors:
1. establishing suitable security measures which in particular prevent the loss or abuse of TT Keys;
  2. the separate safekeeping of customers' Tokens and business assets of the TT Protector; and
  3. the clear assignment of customers' Tokens;
  4. the execution of customers' orders in line with agreements;
  5. the maintenance of the services in the event of interruptions (business continuity management);
- g) for TT Exchange Service Providers:
1. the disclosure of comparable market prices of the traded Tokens;
  2. the disclosure of the purchase and sale prices of the traded Tokens;
- h) for TT Verifying Authorities, the use of suitable measures which ensure that the verification services it offers are rendered reliable;
- i) for TT Price Service Providers:

1. the transparency of the published prices;
2. the avoidance of conflicts of interest when setting prices;
3. the disclosure of information to affected users regarding transactions concerning related parties.

k) for TT Identity Service Providers:

1. the use of suitable measures that allow for the identity of the person possessing the right of disposal to be established; in doing so, it must be ensured that:
  - aa) for natural persons or natural persons serving as a representative of a legal person who are physically present, their identity is determined based on official photo identification, or by other evidence that has been or is to be a document of equivalent reliability; moreover, for representatives of legal persons, it must be ensured that the necessary power of representation has been determined;
  - bb) for natural persons or legal persons not physically present, other identification methods are to be applied that allow for identification equivalent to under letter aa) to be determined;
2. the specific assignment of TT Identifiers to the lawful holder;
3. the secure storage of customer data.

2) The obligations arising from the internal control mechanisms under (1) must always be complied with.

## **2. Registration procedure**

### Article 18

#### *Registration application*

1) The registration application pursuant to article 12 must include the following information and documents:

- a) name or company and address of the applicant;
- b) information about the intended TT Service;
- c) information about the TT Systems to be used during the planned TT Service;
- d) information about the legal nature of the applicant, in the event that the applicant is a legal entity;
- e) evidence that the requirements pursuant to articles 13 to 17 have been met;
- f) further information and documents at the request of the FMA if necessary to assess the registration application.

2) The registration application and the information and documents under (1) may be submitted in electronic form to the FMA. The FMA may demand certificates to be submitted in the original, or that they be submitted in notarised or apostilled form.

3) Changes in the information and facts under (1) must be reported to the FMA without delay. This notification to the FMA must be made prior to any public announcement.

4) The FMA may waive the submission of certain information and documents under (1) if it already has access to them, in particular because:

- a) the applicant already has authorisation according to the Financial Market Supervision Act;
- b) the applicant is already registered to render a TT Service other than the one he is applying for; or
- c) the application has already been registered for the same TT Service.

5) The government shall regulate the registration application in more detail, in particular the evidence under (1)(e) by means of ordinance.

#### Article 19

##### *Entry into the TT Service Provider Register*

1) Based on the complete application and the information respectively documents submitted, the FMA must verify whether the registration requirements have been met.

2) The FMA must decide on the full application within three months.

3) If all registration requirements have been met, the FMA must enter the applicant into the TT Service Provider Register (article 23) and inform the applicant of the entry by sending an excerpt from the TT Service Provider Register. The FMA may carry out registration subject to conditions and obligations.

4) If the registration requirements are not met, the FMA must establish this within the period specified in (2), notwithstanding a procedure according to article 46 prohibiting the exercise of the TT Service in question.

5) The TT Service applied for may only be exercised for the first time after having been entered into the TT Service Provider Register.

### **3. Expiration and removal**

#### **Article 20**

##### *Expiration of Registration*

1) Registration in accordance with article 19 will expire if:

- a) the business has not commenced within a year;
- b) the business activity was not carried out for more than one year;
- c) the registration is waived in writing;
- d) bankruptcy proceedings are commenced in respect of the TT Service Provider with legal effect, or are rejected due to insufficient assets to cover the costs pursuant to article 10(3) KO; or
- e) the TT Service Provider's company has been deleted from the Commercial Register.

2) The expiration of a registration must be published in the Official Journal at the expense of the TT Service Provider, and noted in the TT Service Provider Register in accordance with article 23.

#### **Article 21**

##### *Removal of the registration*

The FMA must remove a registration pursuant to article 19 if:

- a) the registration requirements are no longer met;

- b) the TT Service Provider deleted the registration as a result of false information or in any other way or the FMA was unaware of the essential circumstances;
- c) a TT Service Provider systematically or seriously violates its legal obligations; or
- d) a TT Service Provider does not comply with the FMA's requests to restore the lawful status.

2) The revocation of a registration must be provided and communicated to the TT Service Provider in question. After becoming legally effective the revocation must be published in the Official Journal at the expense of the TT Service Provider and must be noted in the TT Service Provider Register in accordance with article 23.

## Article 22

### *Effect of the expiration and removal of the registration*

1) With the expiration or removal of the registration pursuant to articles 20 and 21, the TT Service Provider must cease activity immediately.

2) The TT Service Provider must take the necessary precautions to ensure the interests of its clients are not impaired by the discontinuation of activities, and further, inform the FMA of these precautions immediately by providing a relevant description of the same precautions.

3) If the FMA recognises that the precautions are insufficient, it must monitor implementation, and if necessary, commission an audit office to monitor implementation. The associated costs will be borne by the affected TT Service Provider.

#### **4. TT Service Provider Register**

##### **Article 23**

##### *Maintenance of the TT Service Provider Register*

1) The FMA must maintain a publicly accessible register in which the following information must be entered:

- a) the TT Service Providers registered in Liechtenstein, citing the date of registration;
- b) the scope of the registered TT Services pursuant to article 12 including any possible requirements citing the date of the entry of the TT Service in question;
- c) the expiration or removal of the registration pursuant to articles 20 and 21.

2 The FMA must verify entries under (1) based on a notification pursuant to article 18(3) and update them immediately if necessary.

3) The FMA must make the TT Service Provider Register available free of charge on its website. In addition, the FMA must grant any person access to the TT Service Provider Register at its physical office location, so long as technically feasible.



## 5. Exercising of business activity

### Article 24

#### *Designation Protection*

1) Only registered TT Service Providers may make use of designations indicating activity as a TT Service Provider in any statement of company business purpose or in the company's advertising.

2) The government can further regulate details by ordinance.

### Article 25

#### *Safeguarding Requirements*

1) Tokens held in a trust or in the name of the customer must be considered third-party assets in the event of enforcement, composition agreement proceedings, and in the event that the TT Service Provider becomes bankrupt; and shall be sorted in favour of the customer, subject to all claims of the TT Service Provider against the customer. The Tokens must be protected against claims of the TT Service Provider's other creditors, particularly in the event of bankruptcy, in order to protect the users. Tokens must be stored separately from the TT Service Provider's assets at all times.

2) TT Keys which a TT Service Provider holds or keeps in safe custody for a customer in the TT Service Provider's own name or in the client's name must be considered third-party assets in the event of enforcement, composition agreement proceedings, and in the event that the TT Service Provider becomes bankrupt; and shall be sorted in favour of the customer, subject to all claims of the TT Service Provider against the customer. The Tokens must be protected against

claims of the TT Service Provider's other creditors, particularly in the event of bankruptcy, in order to protect the users.

3) Upon request, during ongoing business operations, a TT Service Provider must present proof to the FMA showing that he has taken sufficient measures to comply with the requirements specified in (1). If the evidence is not provided or if the measures are insufficient, the FMA shall request that TT Service Provider furnish the necessary evidence, or take suitable and necessary precautions to remedy the existing defects. This must be carried out in accordance with an appropriate deadline set by the FMA. If the supporting documents are not submitted or precautions are not taken at all, or within the time frame stipulated by the FMA, the FMA may take further measures, in particular, those set out in article 43(5).

4) In the event of enforcement against his TT Service Provider, the user has the right to appeal (article 20 of the Execution Law), if the enforcement relates to the Tokens secured in accordance with (1) or the TT Keys secured in accordance with (2). Under the same requirements, in the event of bankruptcy of the TT Service Provider, the user has the right to have his Tokens segregated from the assets of the TT Service Provider (article 41 of the Bankruptcy Rules (KO)).

## Article 26

### *Storage of Records and Supporting Documents*

1) TT Service Providers must keep relevant records and supporting documents for supervisory purposes for at least ten years.

2) More specific legal obligations remain unaffected.

Article 27

*Outsourcing Functions*

- 1) The outsourcing of important operational functions is permitted if:
  - a) the quality of the internal control of the TT Service Provider is not significantly impacted;
  - b) the obligations of the TT Service Provider remain unchanged according to this Act; and
  - c) the registration requirements according to this Act are not undermined.

2) In this context, an operational function is particularly important if it, only partially fulfilled or neglected, would significantly affect the TT Service Provider's ongoing compliance with its obligations under this Act or its financial performance.

3) A TT Service Provider outsourcing functions must take adequate precautions to ensure that the requirements of this Act are met.

4) Special statutory regulations on the outsourcing of functions remain reserved.

Article 28

*Reporting obligations*

- 1) TT Service Providers must inform the FMA immediately of:
  - a) all changes with regard to the registration requirements;
  - b) the cessation of business activities;
  - c) the removal of the TT Service Provider from the Commercial Register.

2) TT Service Providers must inform the FMA of all information about its business activity required to exercise supervision.

3) The government shall regulate reporting obligations, in particular the frequency and content of the notifications under (2) in more detail by means of an ordinance.

#### Article 29

##### *Publication obligations*

1) TT Service Providers must publish the following in a way that can be accessed by the public at any time:

- a) information about the TT Systems it uses;
- b) a declaration on the suitability of the TT Systems it uses for the application purposes in question;
- c) information about any possible change in a TT System, including a relevant justification.

### **6. Basic information for Token Issuance**

#### Article 30

##### *Obligation to prepare, report and publish basic information*

Subject to (31), before issuing Tokens Token Issuers must:

- a) prepare basic information according to the following provisions;
- b) publish the basic information in an easily accessible way; and
- c) report the Token Issuance to the FMA.

Article 31

*Exceptions*

1) The obligations pursuant to article 30(a) and (b) shall not apply for public offerings of Tokens if:

- a) all recipient parties demonstrably declare that they waive the basic information before acquiring the Token;
- b) the offer is geared towards fewer than 150 users;
- c) the sale price of the total issue does not exceed 5 million Francs or the corresponding equivalent in another currency, where this upper limit is to be calculated over a period of twelve months; or
- d) there is already an obligation to publish qualified information about the public offering of Tokens according to other laws.

2) No additional basic information needs to be published for any later public resale of Tokens if:

- a) the basic information pursuant to article 30 has already been published; and
- b) the issuer or the person responsible for preparing the basic information has approved its use in a written agreement.

Article 32

*Form and language of the basic information*

1) Basic information must be prepared and published in a way that is easy to understand.

2) Basic information can be prepared and published in one or several documents.

3) If basic information consists of several documents, then the Token Issuer must prepare and publish a brief, easily understandable summary with information about the Token Issuer and the Tokens to be issued.

4) Basic information must be prepared and published in German or English.

### Article 33

#### *Content of the basic information*

1) Basic information must in particular include the following:

- a) information about the Tokens to be issued and associated rights;
- b) the name of the TT system used;
- c) a description of the purpose and nature of the legal transaction underlying the Token Issuance;
- d) a description of the purchase and transfer conditions for the Tokens;
- e) information about the risks associated with purchasing the Tokens;
- f) for the issuance of Tokens which represent rights to property:
  - 1. evidence of a registered Physical Validator regarding ownership of the property; and
  - 2. a confirmation from a registered Physical Validator that the rights registered in the issued Tokens are also enforceable in line with the basic information.

2) The basic information moreover includes a summary which contains brief and generally understandable essential information in the language in which the basic information was originally prepared. The summary must also include warnings that:

- a) it is to be understood as an overview of the subsequent basic information;
- b) the recipient party must read all of the basic information before purchasing; and
- c) persons who have assumed responsibility for the summary, including its translation, or who prepare the summary or translation can only however be made liable in the event that the summary is misleading, incorrect or inconsistent if read together with other parts of the basic information.

3) The basic information must include the names and roles (and, for legal persons, the company and headquarters) of those who are responsible for the content. The basic information must include a declaration by these persons that the information is correct to the best of their knowledge and that no significant information has been left out.

4) The basic information must also include the names and roles (and, for legal persons, the company and headquarters) of those who are responsible for the technical and legal functionality of the Token.

5) The Token Issuer must put an issuance date on the basic information and ensure it cannot be amended through suitable measures.

6) The government may regulate the content of the basic information in more detail by means of an ordinance.

*Addendum to the basic information*

1) Any new material fact or every material error or inaccuracy, with regard to the basic information that is determined after the basic information is first published must be named in an addendum to the basic information.

2) In addition, the summary and any translations of the summary must be supplemented by the information included in the addendum.

3) The government may regulate the addendum to the basic information in more detail by means of an ordinance.

Article 35

*Liability*

1) If any facts in the basic information that is to be prepared according to this Act are incorrect or incomplete, or if the basic information in accordance with these provisions was not prepared, the persons responsible under articles 33(3) and (4) shall be liable to every user for damages that arise as a result, provided they do not demonstrate that they took the due care of a prudent businessman when preparing the basic information. Only damage directly suffered is considered to be damage, not including loss of profit.

2) The persons named in (1) shall also be liable for their vicarious agents and employees, provided they do not demonstrate that they acted with due care according to the circumstances in their selection, instruction, and supervision.

3) Liability under (1) and (2) cannot be waived or restricted in advance to the detriment of users in the event of intent or gross negligence.



4) Liability shall only be borne for information in the summary including its translations if they are misleading, incorrect or inconsistent in connection with other parts of the basic information; or if they do not convey all material information. The summary must include a clear warning in this respect.

#### Article 36

##### *Severability*

If several persons are liable to pay compensation for a damage, each of them shall be held jointly and severally liable with the others so long as the damage is personally attributable to their own negligence and circumstances.

#### Article 37

##### *Jurisdiction*

The Court of Justice shall have jurisdiction for claims of the transferee of a Token regarding the legal relationship with the Token Issuer with headquarters within the country.

#### Article 38

##### *Statute of limitations*

Any claim for damages against the persons who are responsible in accordance with the above provisions will be barred by the statute of limitations one year from the date on which the cause of action accrues, the cause of action accruing on the date the injured party is both aware of the damage and the identity of the party liable for the damage, expiring regardless, ten years from the date of the harmful act.

**B. Supervision**

## Article 39

*Jurisdiction*

The Financial Markets Authority (FMA) is responsible for the supervision of TT Service Providers and the execution of the associated statutory provisions.

## Article 40

*Official Secrecy*

1) The FMA, any other persons consulted by these authorities and bodies and all representatives of public authorities shall be subject to official secrecy without any time limits with respect to the confidential information that they gain knowledge of in the course of their official activities.

2) Confidential information within the scope (1) may be transmitted in accordance with this Act or special statutory provisions.

3) If bankruptcy or liquidation proceedings have been initiated against a TT Service Provider by the decision of a court, confidential information which does not relate to third parties may be disclosed in civil law proceedings, if this is necessary for the proceedings concerned.

4) Without prejudice to cases covered by the requirements of criminal law, the FMA, all other administrative authorities, courts and bodies, natural persons or legal entities may only use confidential information that they receive in accordance with this Act only for purposes of fulfilling their responsibilities and tasks within the scope of this Act, or for purposes for which the information was given, and/or in the case of administrative and judicial proceedings that specifi-

cally relate to the fulfilment of these tasks, provided this is required to do so. If the FMA, another administrative authority, court, body, or a person transmitting information, gives its consent; then the authority receiving the information may use it for other financial market supervision purposes.

#### Article 41

##### *Cooperation Between National Authorities and Agencies*

The FMA works with other competent national authorities and agencies provided this is required to fulfil its duties under this Act.

#### Article 42

##### *Processing and transferring personal data*

1) The FMA and other competent national authorities and agencies may process personal data, including personal data regarding criminal sentences and offences of the persons subject to this Act, or have such processed externally, if this is necessary in order to fulfil their duties under this Act.

2) They may send personal data to each other or other competent authorities in other EEA member states, if this is necessary in order to fulfil duties under this Act.

3) They may send personal data to the competent authorities of third-party states if the data protection requirements under chapter V of Regulation (EU) 2016/679 have been met in addition to the requirements under (2).

## Article 43

### *FMA duties and authorisations*

1) In the course of its supervision, the FMA monitors compliance with the provisions of this Act and its associated ordinances.

2) The FMA is responsible for the following duties in particular:

- a) registering TT Service Providers and the removal of registrations;
- b) issuing information about the application of this Act or another Act listed in article 5(1) FMAG (Financial Markets Supervision Act) for clearly determined facts in connection with Trustworthy Technology;
- c) maintaining the TT Service Provider Register in accordance with article 23;
- d) the prosecution of contraventions in accordance with article 47(2).

3) The FMA has all necessary authority to perform its duties and may, in particular:

- a) require TT Service Providers to provide all information and documents required for the execution of this Act;
- b) order or carry out extraordinary audits;
- c) make decisions and ordinances;
- d) issue legally binding decisions and rulings;
- e) carry out on-site inspections of TT Service Providers; and
- f) correct false information that has been published by naming the TT Service Provider involved and issue warnings;
- g) temporarily prohibit the exercising of a TT Service.

4) If the FMA becomes aware of violations of this Act or of other deficits, it shall take the measures necessary to bring about a lawful state of affairs and to eliminate the deficits.

5) The FMA may assign an expert to a TT Service Provider to act as its observer if the interests of users or creditors appear to be acutely endangered by mismanagement. Appointed external audit offices may be entrusted with this responsibility. The observer shall monitor the activities of the governing bodies, in particular the implementation of the measures ordered, and shall report to the FMA on an ongoing basis. The observer shall enjoy the unrestricted right to inspect the business activities and the books and files of the TT Service Provider. The cost of the supervisor must be borne by the TT Service Provider, insofar as a reasonable relationship exists between the work associated with the activity and its expenses.

6) If there is reason to assume that a person is rendering TT Services without authorisation pursuant to this Act, the FMA may demand information and documents from the person concerned if this person is a subordinate person. In urgent cases, the FMA may order the immediate cessation of the activity without prior warning or imposition of a deadline.

7) The costs incurred due to misconduct shall be borne by those responsible in accordance with article 26 of the Financial Market Supervision Act.

8) The government can further regulate details by ordinance.

Article 44

*Supervision taxes and fees*

The Supervision taxes and fees shall be levied in accordance with the Financial Market Supervision Act.

**C. Proceedings and Legal Remedies**

Article 45

*Proceedings*

To the extent not otherwise specified in this Act, the provisions of the National Administration Act (LVG) shall apply to proceedings.

Article 46

*Legal remedy*

1) Decisions and decrees of the FMA may be appealed within 14 days of service to the FMA Complaints Commission.

2) Decisions and decrees of the FMA Complaints Commission may be appealed within 14 days of service to the Administrative Court.

**D. Penal provisions**

Article 47

*Offences and infractions*

1) The following persons shall be penalised by the District Court for offences with up to one-year imprisonment or a fine of up to 360 daily rates:

- a) those who render TT Services requiring registration in a manner contrary to article 12;
- b) those who use a designation contrary to article 24 which suggests activity as a TT Service Provider;
- c) those whose registration as a TT Service Provider expired due to false information or other illegal matters; or
- d) those who systematically violate their legal obligations as a TT Service Provider in a serious manner.

2) If the action does not constitute a criminal offence within the jurisdiction of the courts, TT Service Providers shall be fined by the FMA by up to 100,000 Francs due to an infraction if:

- a) they do not comply with the minimum capital requirements under article 16;
- b) they violate the obligations arising from the internal control mechanisms under article 17;
- c) they violate the reporting obligations under article 18(3) and article 28;
- d) they do not comply with the FMA requirements and conditions associated with registration pursuant to article 19(3);
- a) they violate the security obligations pursuant to article 25;
- f) they do not keep records, or keep insufficient records or do not store supporting documents contrary to article 26;
- g) they outsource important operational functions without meeting the requirements pursuant to article 27;
- a) they violate their publication obligations pursuant to article 29;

- i) they violate the preparation, publication and reporting obligations for basic information pursuant to article 30 et seq.;
- i) they fail to comply with a decree or order issued to them by the FMA with reference to the threat of punishment under this article.

3) The FMA must impose fines against legal persons if the infractions under (2) are committed in execution of the course of business of legal persons; (offences) by persons who have either acted alone or as a member of the Administrative Board, Management Board, or Supervisory Board of the legal person; or another management position within the legal person, based on which they:

- a) are authorised to outwardly represent the legal person;
- b) exercise supervisory powers in a management position; or
- c) otherwise exercise significant influence over the management of the legal person.

4) For infractions under (2) committed by the employees of the legal person, even if not culpable, the legal person is also responsible if the infraction was enabled or significantly facilitated as a result of the persons named in (3) failing to take the necessary and appropriate measures to prevent such offences.

5) The responsibility of the legal person for the offence and the punishability of the persons named in (3) or the employees named in (4) due to the same offence are not mutually exclusive. The FMA may refrain from pursuing a natural person if a fine has already been imposed on a legal person for the same violation and there are no other circumstances that oppose refraining from pursuing the natural person.



6) In the event of negligent conduct, the upper penalty limits in (1) and (2) above shall be halved.

#### Article 48

##### *Responsibility*

Where violations are committed in the business operations of a legal person, the penal provisions shall apply to the members of management and other natural persons who acted or should have acted on its behalf. With all persons, including the legal entity, shall, however, be jointly and severally liable for monetary penalties, fines, and costs.

#### Article 49

##### *Announcing sanctions; binding effect of convictions*

1) The FMA may announce the imposition of lawful punishments and fines at the expense of the party concerned if this fulfils the purpose of this Act and is and proportionate.

2) A conviction under this Act shall not be binding for the civil court judge with regard to the assessment of guilt, unlawfulness, and determination of damages.

### **IV. Transitional and final provisions**

#### Article 50

##### *Transitional provisions*

1) Persons who render a TT Service requiring registration pursuant to article 12 at the time that this Act comes into force undertake:

- a) to exercise their business activity according to articles 24 to 28; and
- b) to apply for the entry into the TT Service Provider Register to the FMA within a period of twelve months after this Act comes into force; otherwise, the right to render TT Services under this Act shall expire.

2) The provisions regarding the basis for Tokens under civil law according to chapter II may also be applied by the parties for Tokens that were generated before this Act came into force according to article 3(2)(b).

3) The provisions on the basic information for Token Issuance according to articles 30 to 28 shall apply to Tokens that are publicly offered for the first time after this Act comes into force.

#### Article 51

##### *Entry into force*

Provided that the referendum deadline expires unutilised, this Act shall enter into force on... (1/month/year), otherwise on the day after the announcement.

## 1.2 Amendment of the Due Diligence Act (SPG)

### Law

of ...

### on the amendment of the Due Diligence Act

I hereby grant My consent to the following resolution adopted by Parliament:

#### I.

#### Amendment of Existing Law

The Law of 11 December 2008 on Professional Due Diligence in the fight against money laundering, organised crime and terrorist financing (Due Diligence Act, SPG) Liechtenstein Law Gazette 2009 No. 47, in its current version, is amended as follows:

article 2(1) letters l, l<sup>bis</sup>, l<sup>ter</sup>, z<sup>bis</sup>, z<sup>ter</sup> and z<sup>quater</sup>

1) The following definitions are established for the purposes of this Act:

- l) “Exchange Bureau”: natural or legal persons whose activity lies in the exchange of legal tender at official exchange rates;
- l<sup>bis</sup>) “TT Exchange Service Provider”: natural or legal persons whose activity lies in the exchange of virtual currencies or Payment Tokens for legal tender or other virtual currencies or Payment Tokens, and vice versa;

- l<sup>ter</sup>) “Payment Tokens”: a Token pursuant to article 2(1)(d) TTTA;
- z<sup>bis</sup>) “Virtual Currency”: a digital representation of a value that was not issued or guaranteed by any central bank or public body, that is not inevitably pegged to a legally established currency, and that does not have the legal status of a currency or money; but that is accepted by natural or legal persons as means of exchange which can be transferred, saved and traded electronically;
- z<sup>ter</sup>) “Supplier of Electronic Wallets”: natural or legal persons who offer services to safeguard TT Keys on behalf of their customers in order to keep, save or transfer Virtual Currencies or Payment Tokens;
- z<sup>quater</sup>) “Operators of Trading Platforms for Virtual Currencies or Payment Tokens”: natural or legal persons who operate trading platforms via which their customers conclude an exchange of Virtual Currencies or Payment Tokens for legal tender or other Virtual Currencies or Payment Tokens and vice versa and whose activity goes beyond mere brokerage without the involvement of payment flows.

Article 3(1)(q) to (u) and (3)(h).

1) This Act applies to persons subject to due diligence. These are:

- q) Persons who trade goods, provided payment is in cash, Virtual Currency, or Payment Tokens; and the amount is 10,000 Francs or more regardless of whether the transaction takes place in a single operation or several operations between which there appears to be a connection;
- r) TT Service Providers requiring registration pursuant to article 2(1)(l) and (n) to (r) TTTA;

- s) Token Issuers not requiring registration with headquarters or place of residence in Liechtenstein who issue Tokens on their own behalf, or in a non-professional capacity on behalf of their client; if they process transactions of 1,000 Francs or more, regardless of whether the transaction takes place in a single operation or several operations between which there appears to be a connection;
- t) Operators of Trading Platforms for Virtual Currencies or Payment Tokens;
- u) Suppliers of Electronic Wallets.

3) The following persons subject to due diligence must report the commencement of their activity to the competent supervisory authority in writing without delay:

- h) Token Issuers under (1)(s)

#### Article 5(2)(g) and (h)

2) Due diligence must be exercised in the following cases:

- g) for TT Service Provider pursuant to article (3)(1)(r), regardless of any thresholds, even if transactions under (b) are involved; (h) remains reserved;
- h) in the case of TT Exchange Service Providers who only operate physical change machines for the settlement of transaction of 1,000 Francs or more, regardless of whether the transaction takes place in a single operation or in several operations between which there appears to be a connection.

Article 9(b)(2)(a)

2a) Persons subject to due diligence pursuant to article 3(1)(r) must use state-of-the-art systems in order to make a risk-based assessment of the history of the relevant Virtual Currencies or Tokens in the relevant TT System (article 2(1)(b) TTTA). The government will arrange the details by means of a Regulation.

Article 16(1)(1)

1) Persons subject to due diligence pursuant to article 3(1)(a) to (i) and (r) who are part of a group must establish strategies and procedures that apply across the group, including data protection strategies and procedures for exchanging information within the group; in order to combat money laundering, organised crime and financing terrorism. ...

Article 23(1)(a)

1) The supervision and implementation of this Act and execution of Regulation (EU) 2015/847 oblige:

- a) the FMA with regard to persons subject to due diligence pursuant to article (3)(1)(a) to (l) and (n) to (u);

Article 31(1)(f<sup>bis</sup>) and (4), introductory sentence

1) Fines of up to 200,000 Francs will be imposed by the supervisory authority due to administrative infractions on any person who deliberately:

- f<sup>bis</sup>) does not carry out the risk assessment pursuant to article 9(a) or does not use the IT-based systems pursuant to article 9(b);

4) If an administrative infraction pursuant to (1)(c) to (n) is committed by a person subject to due diligence pursuant to article (3)(1)(k) to (u) in a severe, repetative, or systematic manner, then the amount of the fine shall be:

## **II.**

### **Entry into force**

This law shall enter into force at the same time as the TT Service Provider Act of....





### **1.3 Amendment of the Financial Market Supervision Act (FMAG)**

#### **Law**

of ...

#### **on the Amendment of the Financial Market Supervision Act**

I hereby grant My consent to the following resolution adopted by Parliament:

#### **I.**

##### **Amendment of Existing Law**

The Act of 18 June 2004 on Financial Market Supervision (Financial Market Supervision Act; FMAG), Liechtenstein Law Gazette. 2004 No. 175, in its current version, is amended as follows:

##### **Article 5(1)(z<sup>septies</sup>)**

Unless specified otherwise by law, the FMA shall be responsible for the supervision and execution of this Law and of the following Laws, including the implementing ordinances issued in association therewith:

z<sup>septies</sup>) Law on Tokens and TT Service Providers (Tokens and TT Service Provider Act; TTTA)

## Article 30(a)(8)

8) The FMA must report the data required to calculate individual supervision taxes by 31 March of the tax year at the latest provided this data concerns supervised persons from the supervised persons categories under Appendix 2 Chapter III Section C, Chapter IV (with the exception of Section c), Chapter V and Chapter IX.

Appendix 1 Section I.<sup>ter</sup>**I.<sup>ter</sup> TT Service Provider**

The fee for completing the following activities pursuant to the TTTA is, for:

- a) carrying out or rejecting the registration as a TT Service Provider: 1,500 Francs;
- b) the registration of every additional TT Service Provider: 700 Francs;
- c) the removal of a registration: 250 Francs;
- d) the expiration of a registration: 250 Francs;
- e) examining a change in the registration requirements: 700 Francs;
- f) issuing of a confirmation of a registration entry: 50 Francs;
- g) inspecting the TT Service Provider Register at the FMA's headquarters: 50 Francs;
- h) issuing information pursuant to article 43(2)(b) TTTA: 2,000 Francs;
- i) carrying out or rejecting the registration for financial intermediaries already authorised by the FMA: 700 Francs;
- k) the issuance of a decree to bring about a lawful state of affairs and eliminate deficits pursuant to article 43(4) TTTA: 1,000 Francs;

- l) the secondment of an expert pursuant to article 43(5) TTTA: 1,000 Francs;
- m) the order of measures in respect of persons who render TT Services without authorisation pursuant to article 43(6) TTTA: 1,000 Francs;
- n) the issuance of a penal order in the event of an infraction pursuant to article 47(2) TTTA: 5,000 Francs. In the case of a warning, the fee is 1,000 Francs;
- o) the issuance of another decree if there is no fee under (a) to (b); depending on the expense and complexity of the decree to be prepared, 500 to 10,000 Francs.

## Appendix 2, Section IX

### **IX. TT Service Provider pursuant to the TTTA**

#### **A. General**

TT Service Providers who are registered for several services must only pay supervision tax for the service generating the highest supervision tax. Supervision tax is not accumulative.

#### **B. Token Issuers pursuant to article 12(1) TTTA**

1. Basic tax for Token Issuers pursuant to article 12(1) TTTA is 1,000 Francs per year.
2. Additional tax is charged at 0.25% of the equivalent value of all cryptocurrencies and monies received during the issuance in Francs. The day of the initial offer is considered the reporting date for the calculation of the exchange rate. The equivalent value as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.

3. For newly registered Token Issuers, the equivalent value of all issues carried out as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 10,000 Francs for Token Issuers pursuant to article 12(1) TTTA.

#### **C. TT Key Depositories**

1. The base tax for TT Key Depositories is 500 Francs per year.
2. The additional tax for TT Key Depositories which exercised activities relevant for due diligence during the tax year shall be 40 Francs per business relationship relevant for due diligence. The number of business relationships relevant for due diligence as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.
3. For newly registered TT Key Depositories, the number of business relationships relevant for due diligence as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 5,000 Francs for TT Key Depositories.

#### **D. TT Token Depositories**

1. The base tax for TT Token Depositories is 500 Francs per year.
2. The additional tax for TT Token Depositories which exercised activities relevant due diligence during the tax year shall be 40 Francs per business relationship relevant for due diligence. The number of business relationships relevant for due diligence as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.

3. For newly registered TT Token Depositories, the number of the business relationships relevant for due diligence as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 5,000 Francs for TT Token Depositories.

#### **E. Physical Validators**

1. The base tax for Physical Validators is 1,000 Francs per year.
2. The additional tax for Physical Validators which exercised activities relevant due diligence during the tax year shall be 40 Francs per business relationship relevant for due diligence. The number of business relationships relevant for due diligence as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.
3. For newly registered Physical Validators, the number of the business relationships relevant for due diligence as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 5,000 Francs for Physical Validators.

#### **F. TT Protectors**

1. The base tax for TT Protectors is 500 Francs per year.
2. The additional tax for TT Protectors which exercised activities relevant due diligence during the tax year shall be 40 Francs per business relationship relevant for due diligence. The number of business relationships relevant for due diligence as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.

3. For newly registered TT Protectors, the number of the business relationships relevant for due diligence as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 5,000 Francs for TT Protectors.

**G. TT Exchange Service Providers**

1. The base tax for TT Exchange Service Providers is 500 Francs per year.
2. The additional tax for TT Exchange Service Providers which exercised activities relevant for due diligence in the tax year is charged at 0.25% of the exchanged cryptocurrencies and monies in Francs. The sum of the exchange amounts as at 31 December of the year preceding the tax year shall be used to calculate the additional tax.
3. For newly registered TT Exchange Service Providers, the sum of the exchanged cryptocurrencies and monies as at 31 December of the ongoing year shall be used to calculate the additional tax. The tax shall be collected in the following year.
4. The total annual supervision tax per supervised party shall at most be 5,000 Francs for TT Exchange Service Providers.

**H. TT Verifying Authorities**

The annual supervisory tax for TT Verifying Authorities is CHF 250.

**I. TT Price Service Providers**

The annual supervisory tax for TT Price Service Providers is CHF 250.

**K. TT Identity Service Providers**

The annual supervisory tax for TT Identity Service Providers is CHF 250.

**II.**

**Entry into force**

This law shall enter into force at the same time as the TT Service Provider  
Act of....





#### **1.4 Amendment of Persons and Companies Act**

### **Law**

of ...

### **on the amendment of Persons and Companies Act (PGR)**

I hereby grant My consent to the following resolution adopted by Parliament:

#### **I.**

#### **Amendment of Existing Law**

The Persons and Companies Act (PGR) of 20 January 1926, Liechtenstein Law Gazette. 1926 No. 4, in its current version, is amended as follows:

#### **Section 81a (Final Part)**

#### ***G. Uncertificated rights***

1) The debtor can issue rights with the same function as certificated securities (uncertificated rights) or replace fungible securities with uncertificated rights, if the conditions of issue, the articles of association provide for this, or if the beneficiaries have given their consent.

2) The debtor shall keep a ledger of uncertificated rights he has issued, in which the number and denomination of uncertificated rights issued, as well as

the creditors, must be recorded. The ledger may also be managed with the use of Trustworthy Technology pursuant to the TTTA.

3) The uncertificated rights shall come into being upon their entry into the ledger and shall exist in accordance with this entry.

4) The transfer of uncertificated rights or the grant of limited in rem rights shall take place upon entry by the purchaser or the transferee in the ledger of uncertificated rights. If the ledger is managed with the use of Trustworthy Technology pursuant to the TTTA, then the disposal over the uncertified rights shall be exclusively based on the regulations of the TTTA.

5) Anyone who acquires uncertificated rights, or rights to uncertificated rights, in good faith from the person entered in the ledger of uncertificated rights shall be protected in his acquisition, even if the seller was not authorised to dispose of the uncertificated rights.

6) The debtor shall only be obliged to effect payment to the creditor entered in the ledger of uncertificated rights. By making payment due at maturity to the creditor entered in the uncertificated rights ledger, the debtor is released from his obligation, unless he is guilty of malice or gross negligence.

## **II.**

### **Entry into force**

This law shall enter into force at the same time as the TT Service Provider Act of....

## **1.5 Amendment of the Business Act (GewG)**

### **Law**

of ...

### **on the amendment of the Business Act**

I hereby grant My consent to the following resolution adopted by Parliament:

#### **I.**

#### **Amendment of Existing Law**

The Business Act (*Gewerbegesetz* - GewG) of 22 June 2006, Liechtenstein Law Gazette. 2006 No. 184, in its current version, is amended as follows:

#### Article 3(s)

This Act shall not apply to:

- s) the activity of TT Service Providers pursuant to the TTTA

**II.**

**Entry into force**

This law shall enter into force at the same time as the TT Service Provider  
Act of....