Unofficial Translation of the Government Consultation Report and the Draft-Law on Transaction Systems Based on Trustworthy Technologies (Blockchain 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 public consultation.

GOVERNMENT

CONSULTATION REPORT

ON

THE CREATION OF A LAW ON TRANSACTION SYSTEMS BASED ON TRUSTWORTHY TECHNOLOGIES (TT) (BLOCKCHAIN LAW; TT-ACT; VTG) AND THE AMENDMENT OF OTHER LAWS

Ministry for General Government Affairs and Finance

Consultation deadline: 16 November 2018

TABLE OF CONTENTS

SUMMARY

"Blockchain technology" was initially developed for Bitcoin, a private digital monetary system. Blockchain technology functions as a ledger that can securely record financial transactions. The technology can be used for much more than Bitcoin. 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 "assets" such as money digitally, preventing these assets from being copied or manipulated and ensuring that they can be transferred securely between different people. The security of such transactions is ensured not by a complex organisation but rather through purely 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 possibilities presented by blockchain technology are not merely limited to simple transfers of money between private individuals. The technology offers the opportunity for a broad range of financial services. This is noteworthy because it means the creation of digital recording of money 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 for assets 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, exchanges for crypto-currencies, and issuing and trading crypto-securities. Blockchain technology is also used for so-called "initial coin offerings" (ICOs), which represents a new way of funding companies or projects. 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, 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 increasing propagation of blockchain applications has already shown 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. Because blockchain technology is also actively used in Liechtenstein, the government aims to use this Law to clarify the applicable requirements for important activities on blockchain systems in order to improve customer protection and reduce potential reputation risks for Liechtenstein.

In addition, there is currently legal uncertainty regarding business models based on TT systems, which are not subject to financial market legislation, but which involve activities that are very similar to those in the financial sector. With the TT-Act, the government aims to define the minimum requirements for these activities on TT systems and have them registered by the FMA.

The legal classification of elements on TT systems is another focus of this draft. With the "token", the TT-Act introduces a new construct so as to enable the transition of the "real" world to TT systems in a legally secure manner and thus tap the full potential of the token economy. The introduction of the legal construct of the token in Liechtenstein Law makes it necessary to also define other legal aspects, such as ownership, possession and transfer.

To be able to shift the representation of securities from physical certificates to tokens on a TT system, the legal concept of uncertificated rights will be introduced in Liechtenstein Law and, simultaneously, an interface created between securities law and the TT-Act. Uncertificated rights are dematerialised securities which are recorded in a book-entry register rather than being issued as a certificate.

In addition, the TT-Act defines minimum requirements for a TT system in order to increase the efficiency of the token economy by building trust among users.

Because of the enormous potential of the "token economy" for large parts of the economy, the government wants with this Law to increase legal certainty for users and service providers to support the positive development of the token economy in Liechtenstein. By doing so, the government is also responding to the needs of market participants for greater legal certainty in connection with TT systems.

<u>RESPONSIBLE MINISTRY</u>

Ministry for General Government Affairs and Finance

<u>AFFECTED ENTITIES</u>

Liechtenstein Financial Market Authority
Regional court
Public prosecutor's office
Office of Justice
Office of Economy

Vaduz, 28 August 2018

LNR 2018-879

P

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-cast and scalable availability of high-performance computers and data storage as well as enormous progress in the area of artificial intelligence (AI), which 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.).

By contrast, the development of crypto-currency has moved companies away from the traditional transaction system. Crypto-currency (such as Bitcoin) is a digital payment method that is created on the basis of cryptographic principles. The concept behind Bitcoin, which was developed in 2008, set developments in motion, the full effects of which are difficult to assess at present. The “inventor” of Bitcoin (who is only known by the pseudonym Satoshi Nakamoto) wanted to create a monetary and payment system that was completely independent of government currencies, central banks and government-controlled banks. In doing so, he had to solve several problems. First, he had to ensure the stability of the currency. He solved this problem by setting a limit on the amount of money that could be created and by defining clear rules for creating new currency. Another area of difficulty was securely assigning the money to an individual, securely transferring money as part of the payment process and – related to this issue – preventing money from being copied (“double spending problem”). To solve these problems he created the so-called “blockchain”, a transaction protocol that is intended to ensure similar or better security with the help of encryption technology (cryptography) and without a central intermediary (such as a central bank or a bank). A fundamental aspect of this system is that the integrity of the transaction protocol is ensured solely through technology. By contrast, in the banking system an intermediary is responsible for ensuring integrity. Transactions are recorded, encrypted and stored online only. In contrast to the current payment system, in which each participant (e.g. a bank) must maintain its own ledger and reconcile it on a defined date with its interfaces (e.g. correspondence banks), with the blockchain there is only one ledger, but a copy of this ledger is stored in a decentralised manner on all participating computers. That is why these ledgers use what is called “decentralised ledger technology” (or “distributed ledger technology”, “DLT” for short).

Bitcoin has expanded and developed substantially since its invention in 2008. Because of its sharp rise in value in recent years, it has increasingly become an object of investment for specialised investors. As the owner of the currency is not 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 exponentially 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.

In 2017, the FMA was in contact with some 100 FinTechs. Many of these companies have some connection with blockchain technology. While the initial focus here was on payment transactions, the focus has of late shifted towards developing new crypto-currencies in various fields of application, e.g. project financing for the development of a new generation of blockchain. These are usually grouped together under the term "initial coin offerings" (ICO), although they can have very different structures, which affects their financial market and tax 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.

For this reason, the Ministry for General Government Affairs and Finance convened an internal expert group in 2016 that looked at the issue of blockchain technology. The expert group concluded that the significance of blockchain-based transaction systems went well beyond current applications. From the expert group's perspective, blockchain has the potential to significantly change large parts of the economy and thus the financial sector. At the same time, they determined that practical regulation would greatly increase legal certainty for all participants and thus favour the development of this innovation. For this reason, the expert group proposed a regulatory concept that the Ministry for General Government Affairs and Finance has adopted in this draft.

2. GROUNDS FOR THE DRAFT

2.1 Main features of blockchain technology

"Blockchain" generally refers to a new software technology based on mathematical models for processing transactions efficiently. Exchange transactions have long formed the basis of the economy – the simplest form is the private exchange of a good for money carried out through personal contact and a contract. Specialised trading systems were developed in order to be able to exchange goods at a distance between two parties who do not know each other directly. Examples include payment transaction systems and securities trading systems. With these traditional trading systems, the buyer and seller are connected and the transaction completed with legal certainty by one or more intermediaries (see Figure 1). This system requires a high degree of standardisation and a high level of requirements in terms of intermediary quality. To ensure quality and create trust, these intermediaries are supervised by the state. Each intermediary maintains a ledger in order to book transactions securely and ensure they are assigned to customers. The reconciliation of the various ledgers, internal processes and government oversight are time-consuming and costly, which is why these trading systems only make sense for certain assets.

By contrast, blockchain offers a transaction system that can be used without the need for quality assurance by intermediaries and without government oversight. Quality is ensured through a combination of encryption technology, the possibilities presented by the Internet and software-based rules to avoid abuses. Thus, blockchain technology and clear rules create the necessary trust to be able to carry out secure transactions.

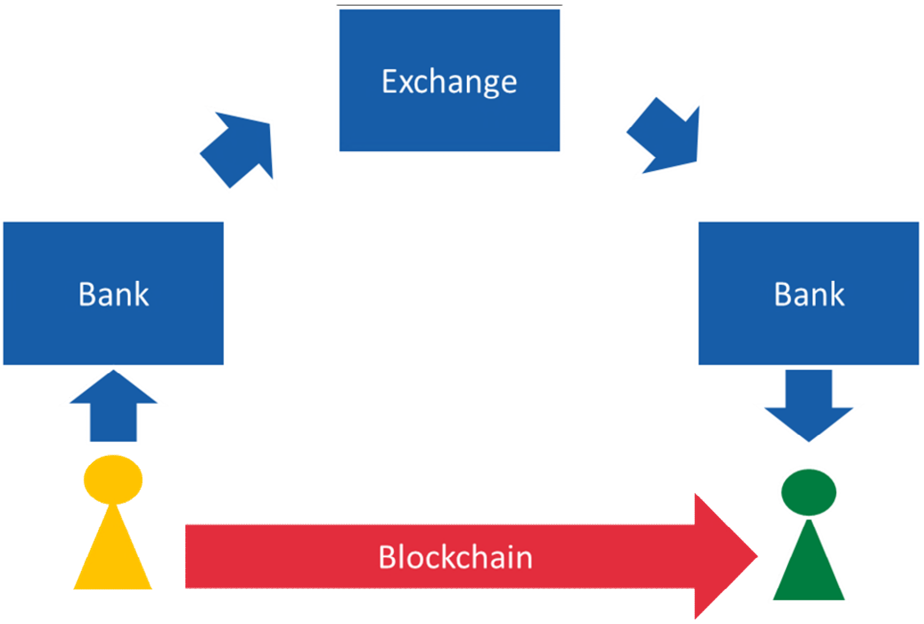


Figure 1: Illustration of the difference between the traditional financial market and blockchain using the example of a securities transaction

The generations of blockchain currently identifiable are based largely on the principle of the decentralised ledger, for which all participants of the transaction system store a copy of the same main ledger recording all transactions, and use it for quality assurance. However, this does not have to be essential for all future generations. The common feature of all systems will be the absence of a central intermediary to ensure the quality of the ledger.

This poses challenges for today's financial market supervision, as the central intermediary is still the link for authorisation and supervision. The traditional supervisory approach does not apply with a blockchain system.

This feature places blockchain systems, as a basic technology, in the same realm as Internet protocols (e.g. TCP/IP), which serve as the foundation of the current Internet and also represent the basis for business models, but which are not themselves operated directly by an intermediary.

Because traditional trading systems are time-consuming and expensive, only limited types of assets are now traded on these systems. Blockchain technology has reduced entry costs substantially. For this reason, it should be assumed that a much broader array of assets will be traded on this type of infrastructure and may be used as the basis for economic processes and the related services.

2.1.1 Structure and functionality of blockchain systems

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

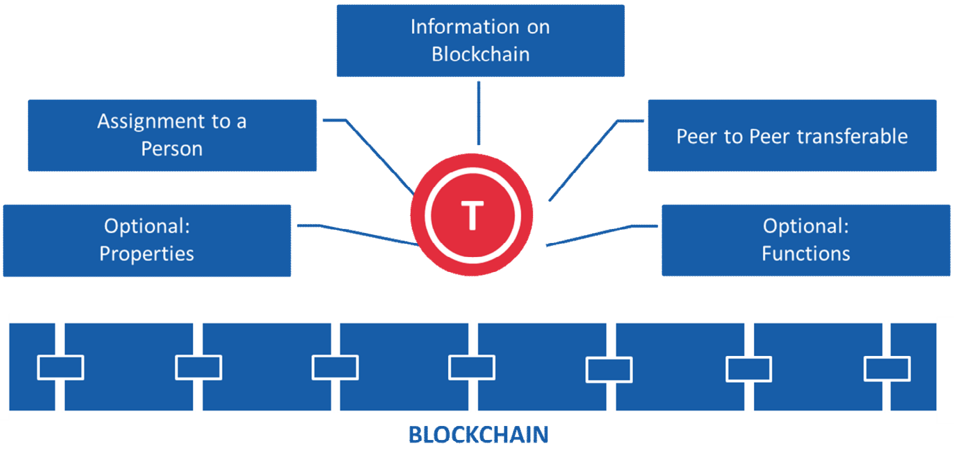


Figure 2: Overview of the typical elements of a blockchain system

The core of a blockchain system is information, i.e. a unique string of characters 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 owner 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.

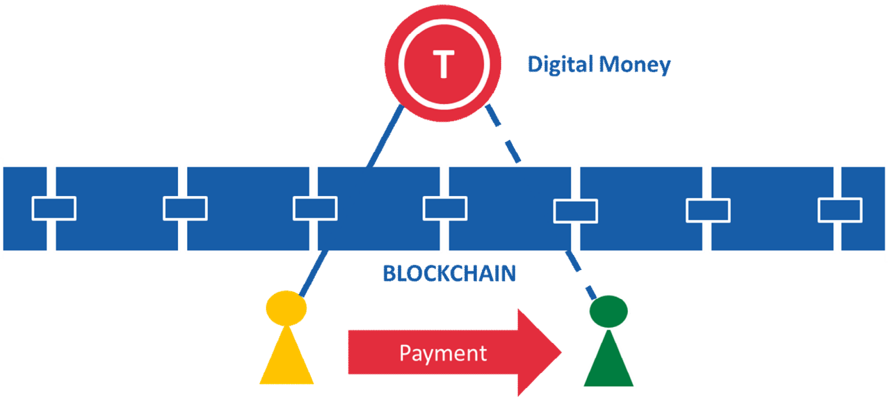


Figure 3: Illustration of a payment using digital currency on blockchain

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 structured like a token, 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 the information is unique. It is therefore not technically possible to make copies. As a result, blockchain technology fulfils the ideal conditions for digitalising money, assets and intellectual property.

On blockchain systems, tokens are clearly allocated to an individual through an entry in the blockchain protocol. This individual has a kind of "address" to which the token is technically allocated. Most current blockchain technologies are based on so-called asymmetrical cryptography, which refers to the address as a "Public Key". As the name indicates, the Public Key is publicly known so that other people can transfer tokens to it. In cryptography, the Public Key is always associated with a "Private Key" that makes it possible to approve or sign transactions.

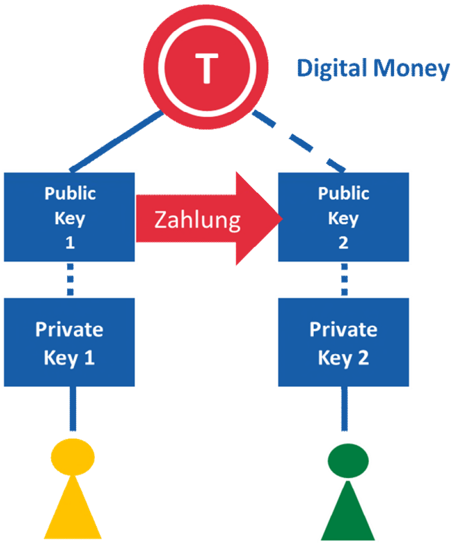


Figure 4: Illustration of the functionality of the blockchain – transferring a token between two Public Keys

To be able to transfer a token, e.g. digital money, from one person to another person, the token (i.e. the unique information) is linked to the new "Public Key" and encrypted with the "Private Key". In this way, transactions are stored in immutable form in the blockchain record and visible to all system participants.

Because the encryption can, in theory, be decrypted with sufficient computing power, blockchain systems rely on additional methods to ensure that the level of security is as high as possible. 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 can be carried out, the majority of participants must confirm that the sender is actually the owner of the token. Only then is the transaction entered in the record and distributed to all participants. 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 practice, be manipulated. Technological progress in computing power will likely be offset by improvements to cryptographic methods.

This description is 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 allocated to a Public Key in the decentralised transaction record. Thus, this information is, in principle, stored in a publicly accessible system like the Internet. Accordingly, the owner of the Private 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 in the form of a QR code, enters the amount and approves the payment. Depending on the blockchain system, the money is allocated to the recipient immediately or within a few minutes.

Figure 5: Public key in 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.

2.1.2 Possible applications of blockchain systems

The original blockchain application is making payments, i.e. transferring private money[1]. 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 blockchain technology 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-

[1] 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. There are two types of currency: currency secured by a real asset (such as gold) and fiat currency (which is not secured by a real asset)

chain systems will likely become much larger: from precious metals, precious stones and commodities, works of art, property and real estate, to used items such as cars, watches and yachts, in the future it may be possible for all economic goods to have a connection with the blockchain. This enormous scope of applications of blockchain systems is usually grouped together under the term “token economy”.

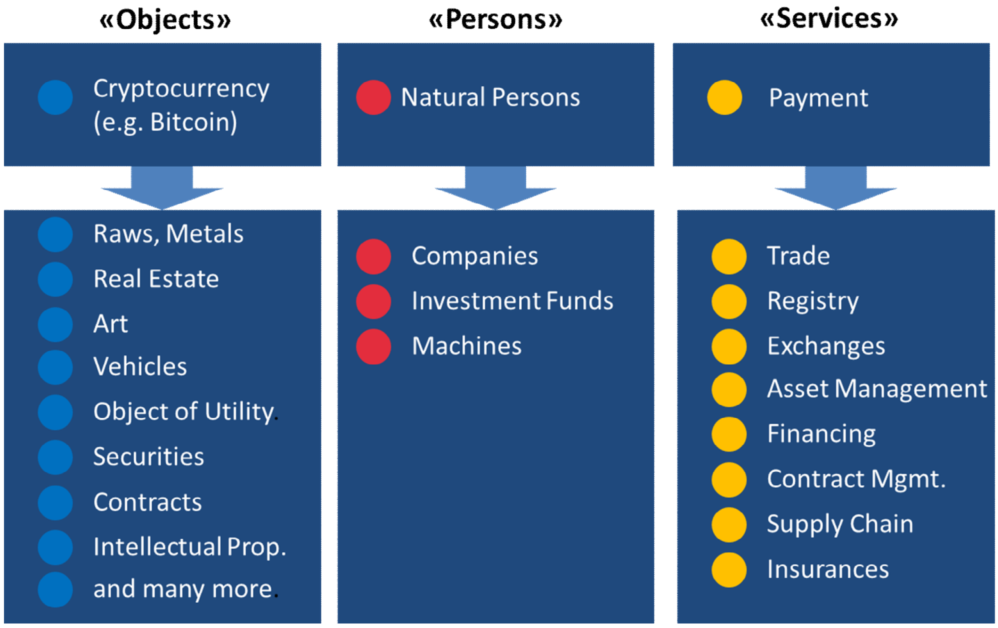


Figure 6: Illustration of scope of application of the “token economy”

Furthermore, blockchain technology will enable an expansion of trading activity. While current efficient transaction platforms may only be used by professional investors and intermediaries, with blockchain the direct and efficient exchange of goods is available to private and retail investors as well. 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.

2.1.3 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:

2.1.3.1 Digital payments

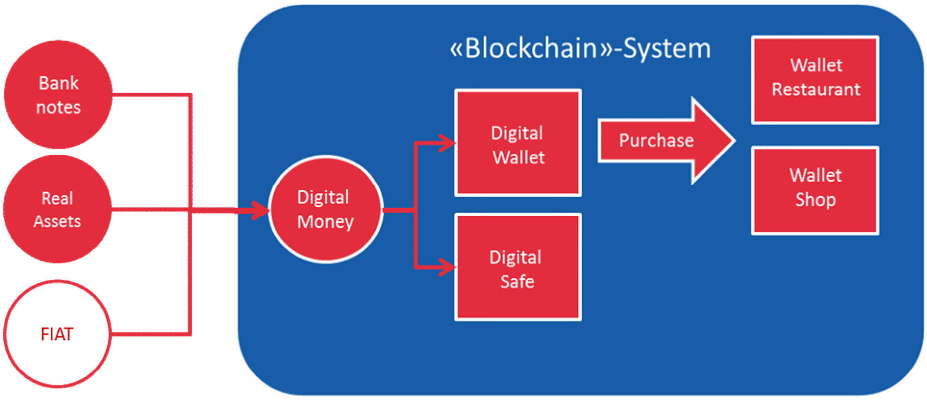


Figure 7: Illustration of applications of digital money

Payments are an obvious application of blockchain systems, one that has already been realised. For digital money to function properly it must have broad acceptance 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 banknotes, i.e. customers have the right to convert digital payment instruments into banknotes at any time

b) the right to exchange legal currencies to a different system (e.g. bank account)

c) if a central bank issues digital payment instruments on blockchain systems: the digital payment instrument immediately assumes the function of the banknote

d) crypto-currency backed by a real asset (e.g. gold), i.e. the holder of the digital money has the right to draw the underlying asset at any time

e) Fiat crypto-currency (e.g. Bitcoin): Classification as a payment instrument is achieved through the system rules and not by a connection with an asset

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

2.1.3.2 Securities, trading and asset management

Securities such as stocks, bonds and derivatives can – as with the traditional transaction system in the financial industry – be transferred or traded via blockchain systems. The applicable financial market regulations for securities and financial instruments continue to apply – irrespective of whether the securities are recorded on the blockchain or not.

Today, the possibility of structuring stocks and corporate bonds in a manner that makes them easy to transfer involves a costly stock listing – with the result that this is used only by large companies. Blockchain systems facilitate greater fragmentation of the value chain process as it relates to securities:

<u>Transferability of stocks and bonds</u>

With blockchain systems, a partial step can be used for a stock listing in place of the full-blown process by recording (existing) stocks or bonds and allocating them to investors, who can then easily transfer them to third parties within the framework of the statutory and special legal regulations.

In principle, the share register can be recorded in the blockchain and could thus reduce the administrative expense for companies.

For investors, the advantage of this intermediary step is that unlisted investment opportunities are also available and, as part of the portfolio, can be transferred to external service providers for asset management. This will expand the investment horizon for both investors and professional service providers.

Corporate financing via shares

The financial system provides companies with the ability to obtain additional capital from a broad circle of investors in the form of an initial public offering (IPO). As this process usually involves a stock listing, it is very expensive and therefore only economically feasible for large to very large companies. The opportunities presented by digitalisation have resulted in the development of so-called "peer-to-peer[2]" forms of financing in recent years (e.g. crowd investing[3] and crowd lending[4]). Blockchain systems (especially Ethereum[5]) have resulted in the option of "initial coin offerings" (ICO), which were developed in order to develop new blockchain technologies, but are now also used for other purposes as well.

[2] In IT, a peer-to-peer network is a network of computers with equivalent rights. This term is also used on crowd investing platforms to designate transactions between equal partners with no intermediary.

[3] In other words: crowdfunding. A way of obtaining financing for projects, products or business ideas from a large number of small investors.

[4] Loans granted by a large number of creditors.

[5] A blockchain technology that enables "smart contracts", i.e. automated contracts.

The issuance of stocks and other equity capital instruments will also be an important factor on blockchain systems in future. Blockchain systems make it possible to reach a large group of investors without the need for a stock exchange. This will help keep financing costs for new equity low. This is very important for both small and medium-sized companies as well as for the investment horizon of investors. Of course, current laws regarding the issuance of stocks also apply on blockchain systems.

Yet stock issues on blockchain systems are not only of interest for direct investments. The services of a stock exchange as part of an IPO, i.e. equal access by a number of investors to the issue and controlled pricing may also be very relevant for investors in future.

Corporate financing via bonds

The same applies for corporate financing via debt capital. While companies can now obtain financing either from banks or from privately or publicly issued bonds, another channel for financing becomes possible via blockchain.

Creation of liquidity/markets

For many investors, it is important for stocks and bonds to be traded regularly so as to ensure that the securities can be sold promptly (liquidity) and a robust price estimate for the sale is available. This requirement will give rise to organised or regulated markets, such as exchanges, MTF and OTF as service providers combining the buying and selling interests of many investors and providing information on blockchain systems as well. Another relevant service may be the provision of aggregated price information and histories, which are important for asset managers in particular.

Traders

Traders will also be needed on blockchain systems to act as service providers for private or institutional investors, ensuring that they receive the best price for the purchase or sale of a security.

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.

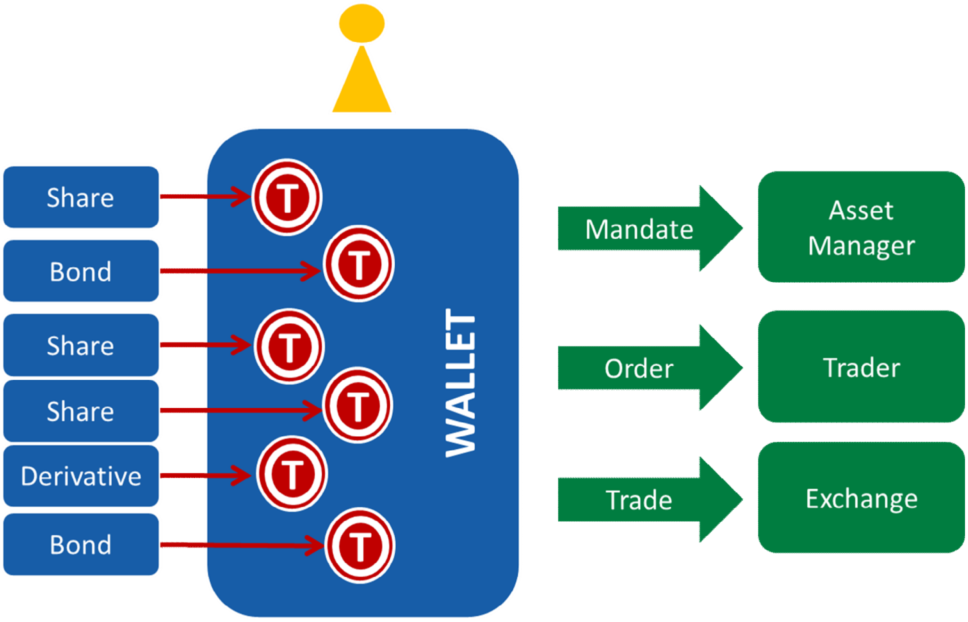


Figure 8: Illustration of the collaboration with financial services providers on blockchain systems

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.

Additional services

Blockchain systems allow for further fragmentation of the value chain. For example, they may result in the development of independent service providers, such as valuation service providers, risk service providers and investment controlling service providers. With blockchain systems, investors can hire such service providers for a wallet directly.

2.1.3.3 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).

2.1.3.4 Funds

Investment funds can be set up on blockchain systems as well. This means that the fund functions like a wallet for storing the collective investments. The fund's unit rights are recorded in the blockchain system and, as a result, these rights generally can be traded. The roles of fund manager, custodian bank and fund administrator continue to be necessary, even though the portfolio is recorded on the blockchain system. These applications are interesting because they enable more cost-effective set-up of, for example, stock exchanges.

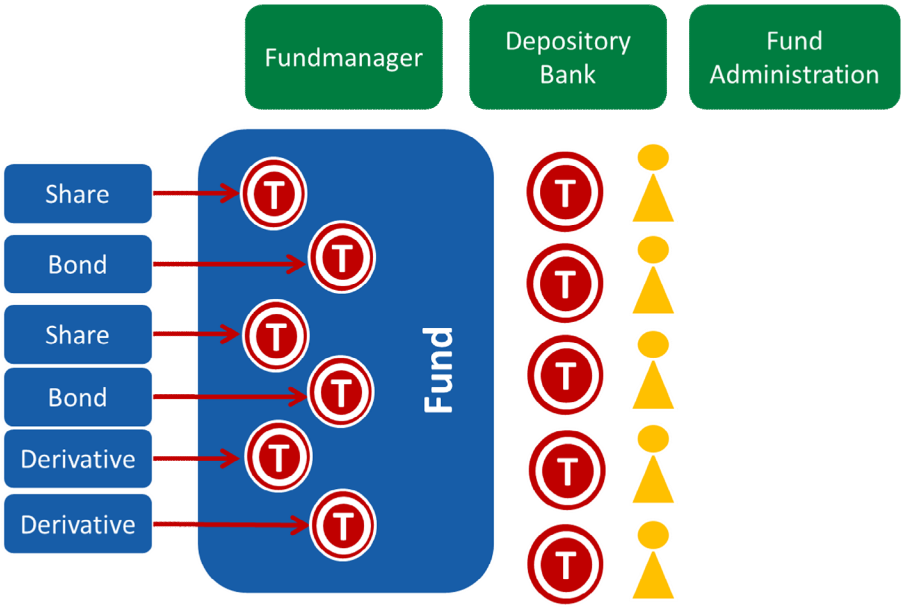


Figure 9: Illustration of a fund structure based on blockchain systems

2.1.3.5 Luxury goods

With blockchain systems, the ownership, licensing and warranty rights for luxury goods can be uniquely recorded in digital form, i.e. they are allocated to a single owner and cannot be copied. 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 stored 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.

2.1.3.6 Music licensing rights

Digital music (e.g. an MP3 file) 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 creates 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.

2.1.3.7 Interfaces with other fields of law

In addition to the TT-Act, 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 TT-Act 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 TT-Act not all applications will be immediately possible, and – if politically desirable – they will have to be implemented in separate projects.

2.2 Need for regulation

2.2.1 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.

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.

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.

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 a white paper and require authorisation.

2.2.2 Reduction of currently known risks

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

Despite the high level of security of the blockchain technology itself, i.e. of the transaction register, it is in principle possible for assets to be stolen. The main point of attack in this regard is the Private Key, which is stored in wallets by either the owners themselves or by service providers. In the past, computer hackers have gained access to wallets and stolen millions on several occasions. As a result, software weaknesses have been corrected and the risk of a similar theft reduced. However, there is – as with every IT system – a race between hackers and software 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, there is the question of how a theft can be claimed legally. The theft of the Private Key means that the thief has an identical copy of the key. In many cases, proof of ownership is no easy task. Even if the thief can be identified, further questions arise about how to reverse the theft. Because the blockchain cannot be manipulated, the theft transaction cannot be simply deleted. If the thief has sold the stolen goods to a third party who purchased them 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.

Nowadays it is not always clear what property status the tokens have in the event of bankruptcy.

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

Another risk is presented by service provider fraud. For one thing, fraud may be committed by stealing the assets that have been entrusted (e.g. in wallets or on crypto-exchanges). 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 Public Keys is completely transparent, yet the owners of Public Keys do not have to be identified. This opens up the potential for abuses, such as money laundering and illegal transactions, on a larger scale than with normal cash transactions, especially because of the low transaction costs. These possibilities must be reined in to combat money laundering and protect Liechtenstein's reputation.

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

Because of the broad range of uses of blockchain systems, there are a number of points of contact with financial market legislation. In some cases, the application of financial market laws is clear, for example, when equity or bond-like instruments are involved. However, there are also many use cases in which considerable assets are recorded on a blockchain system and used as the basis for services, where financial market laws are nevertheless not applicable.

As discussed in the above section, in this connection questions arise, which must be clarified in terms of the legal certainty of customers and users of these systems as well as the reputation of Liechtenstein. For all cases which are not sufficiently covered by current financial market legislation, there must be a legal definition of the general requirements in terms of user protection and legal certainty.

2.2.4 Classification of tokens

The propagation of Bitcoin and other crypto-currencies has led to discussions around the world about how to classify these currencies in terms of financial market and tax law. With the emergence of initial coin offerings (ICOs) it has become clear that too narrow a classification would result in new discussions and thus renewed legal uncertainty in the near term. The range of potential structures of tokens is much greater than that of traditional instruments on the financial market. A clarification of the legal definition of tokens, however, is essential for the legal certainty of all companies which provide services on blockchain systems or plan to do so.

A glance at the potential of the token economy makes it clear that a different approach must be adopted in order to do justice to the potential for innovation and also satisfy the need for legal certainty.

2.2.5 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 it 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 actually receive the digital rights to a product or an asset and that he/she will be able to enforce his/her rights in accordance with 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 (see Figure 10). 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.

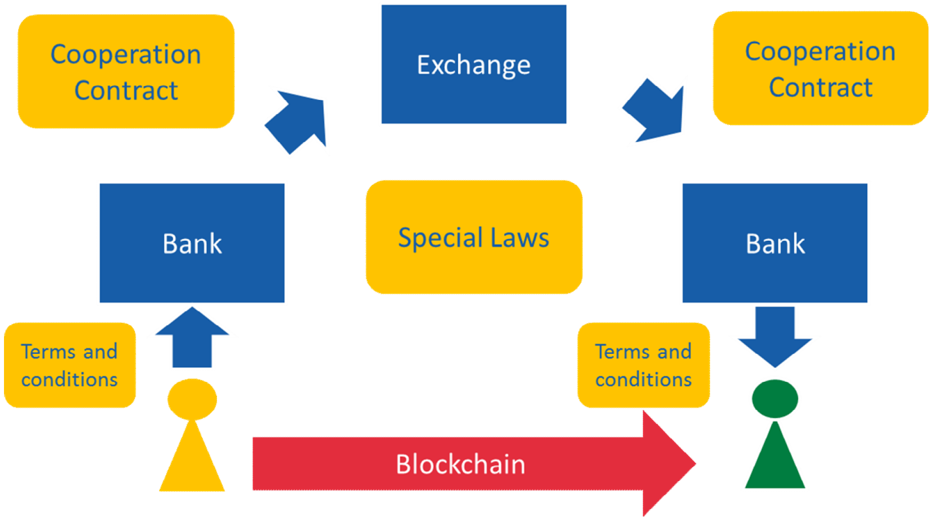


Figure 10: Illustration of the legal certainty of financial transaction systems compared to blockchain systems

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 Internet protocols (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 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 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 "transformation" of the "real" world to 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 theft and misuse, which must also be clarified legally.

Because the token economy can represent not only purely digital assets but also rights to physical objects or contracts, the relationship between the digital rights represented by the tokens and the "real" 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 real 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 needs to have confidence in the reliability and quality of the service provider who, for example, stores the Private Key or token on behalf of the customer, creates tokens and carries out various legal transactions for the customer. 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, and possibly require government registration or even supervision.

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 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 informed 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 TT-Act is a consistent part of these efforts of the government and the FMA to ensure optimal 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 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 coin offerings (ICOs) – 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.

This 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 basic 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. In the token economy, there are many applications with intersections with special laws. Further statutory adjustments are necessary in order to be able to implement these applications, but these will have to be initiated in subsequent projects. Furthermore, it is likely that the application of the Law and the development of the token economy will result in additional questions that will have to be clarified.

2.4 The term “transaction systems on the basis of trustworthy technologies”

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 all 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 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 “cryptosystems” 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 to an owner 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[6] of the main ledger.

The title of the Law “transaction systems based on trustworthy technologies” is therefore intended to cover a view of blockchain systems that is as technology-neutral as possible in order to meet the needs of future generations as well. The government is therefore purposely choosing an abstract definition of the term “blockchain”. The title and the chosen scope thus meet the need for innovation.

The title of this Law 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.

[6] See https://de.wikipedia.org/wiki/Integrität_(Informationssicherheit)

3. MAIN ASPECTS OF THE DRAFT

3.1 Explanation of the basic token model

Today's blockchain ecosystem revolves primarily around crypto-currency and its various applications (payment transactions, ICO). During the implementation of Initial Coin Offerings (ICO) it has also become clear that not only digital money, but also a software usage right or instruments similar to shares can be represented on blockchain systems. This already makes it clear that a legal definition which is mainly about crypto-currency or crypto-securities 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".

The highest level of abstraction, which can cover all possible uses of the "token economy", is the term "right" (legal right). 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 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 construct of the "token", which makes it possible to embody all types of rights on a TT system in the first place. The "token" is therefore a kind of "container" for embodying a right. In this model, a crypto-asset can be depicted as the digital embodiment of a security paper. Crypto-currencies can embody the right to purchase legal tender (e.g.

Swiss francs). The special case of an “empty” container is also possible, and relevant in practice, for example cryptocurrencies without real value collateralisation. In fact the model chosen in this Law can also cover a large number of other application 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 element – the “token” – in the Liechtenstein legal system, there are various aspects which need clarifying, such as ownership and possession, a number of questions relating to delegation to third parties, and the legal connection between the token and the embodied right.

This Law therefore introduces the following basic model (see Figure 11):

- the “token” as a new legal element for embodying rights of all kinds,
- the “Public Key” as an element for allocating the “tokens” (a kind of unique “address”),
- the “Private Key” as an element to dispose of “tokens” which are allocated to a “Public Key”,
- the “holder of the Private Key” as a person who can actually dispose of the “Private Key”,
- the “person authorised to dispose of the Private Key” as the rightful owner of the token, and
- the “delegate of the person holding the right of disposal” as an independent role, for example, in the case of safekeeping of Private Keys.

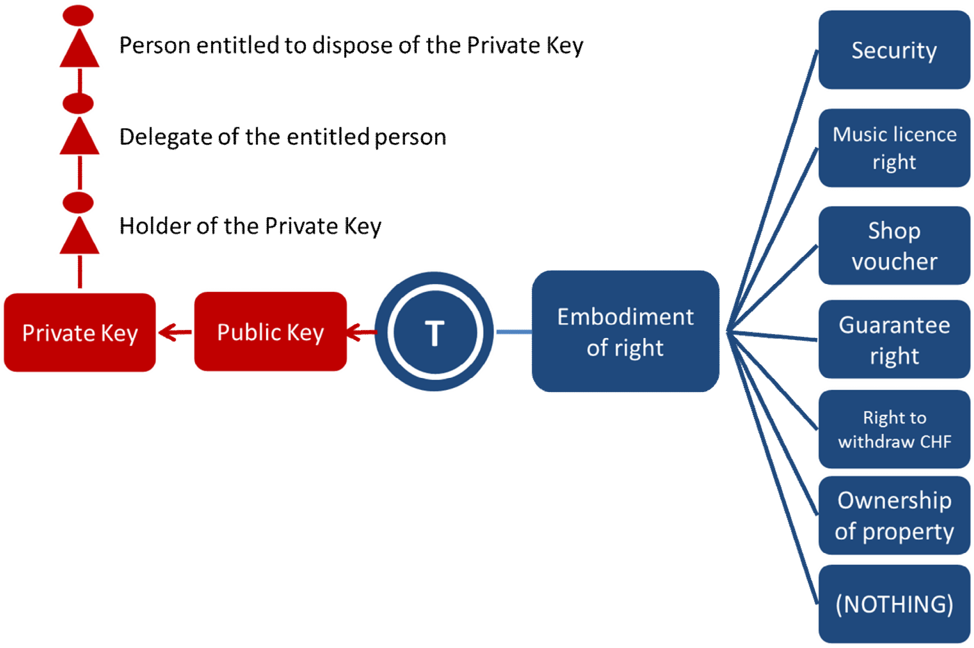


Figure 11: Illustration of the basic model of the token used in the Law, and the various roles

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 element to represent rights of all types on TT systems. A token can embody 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 absolute rights such as intellectual property rights. The basic model – as already mentioned – also permits of empty containers, i.e. tokens without embodied 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 embody 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 legitimation 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 creditor.

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 a fraction of a bitcoin which is allocated to a user in a kind of decentralised accounting system. Nonetheless, the regulations on the disposal over 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 ownership and transfer of ownership of the token, and the legal consequences of the relation to the embodied right, play important roles here.

The abstract definition of the “token” as an independent element used to embody any right requires that one or more persons may own the “token” and transfer it legally to other persons. In terms of ownership, possession and transfer, the “token” certainly bears 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 allocation of assets to their legal entities is possible at any time. Just as in intermediated securities law, however, specific questions present themselves in TT asset law 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 ownership in the TT-Act 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 over the token”. The person entitled to dispose of the token is the holder of full legal responsibility for the token, i.e. he/she may legally dispose of the token and is regarded as the owner of the token, so to speak, and correspondingly also as the owner of the right embodied in the token. According to the current state of knowledge, however, disposal over tokens cannot be exercised directly, but only by way of the Private Key. This means that a duality exists in the right of disposal over a token and over a Private Key. The right of disposal under this Law is linked to a Private Key. The “owner” of 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 “Private 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 prosecute misuse.

Another central challenge of the TT transfer right is 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, not just an empty shell. 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 quite easily ensured by the TT-Act stipulating that the disposal over a token also results in a disposal over the represented right, and that online disposal takes precedence over offline disposal. 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, and takes priority in the event of a collision of interests. 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). If an analogous asset represented by a token is subject to foreign law, the coordinating command of the TT-Act remains ineffective.

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 embodied right as well, and that any other disposal over the right embodied 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 Token Generator 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 embody rights to a token in another token. Examples of this are derivatives, property usage rights (e.g. apartments, cars). It is also possible to embody the rights to so-called TT 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 TT 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 embodiment 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.

The Public Key

On TT systems, tokens are always assigned a unique address, which is defined in the Law as the “Public Key”. It is usual for a number of tokens to be allocated to a single Public Key. The Public Key thus plays a central role in the transmission of tokens between users. Therefore TT wallets always consist of one or more Public Keys, to which and from which tokens can be transmitted.

Public keys 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 Public Keys.

Public keys 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 Public Keys. Smart contracts are automated contracts that can also trigger transactions with tokens.

The Private Key

Another central element is the so-called “Private Key”: Disposal over a Private Key can be gained de facto by way of the tokens allocated to the associated Public Key. The Private Key thus has a very important role in creating legal certainty on a TT system.

The Private Key holder therefore has the actual power of disposal over the token. Yet the holder need not be the person possessing the right of disposal. If a Private Key is stolen, the thief 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 assumes that the holder of the power of disposal is also the person entitled to dispose. In the event of theft, 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 this case the deputy also becomes the person (partially) entitled to dispose of the token. 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 Depositary. The TT Depositary keeps the Private Key on behalf of the customer, for example, to better protect it from theft. Thus the TT Depositary has the de facto power of disposal over the token and also the authorisation to store the Private 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 Private Keys. The owners of the copies will then have the de facto power of disposal over the token. But 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 Public Key to be accessed via several Private 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 Private Key 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 Public Keys. This means that tokens can also be assigned to them, which they can dispose of using Private Keys. So a machine or a smart contract can have the power of disposal and a delegated right of disposal from the persons behind it.

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 encumbering of a right with limited rights in rem (lien, usufruct).

Disposals are not effective unless the person exercising the disposal possesses the right of disposal, i.e. is authorised 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 over tokens. The holder of the token generally has the right to dispose of the token. 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 bankruptcy proceedings are opened with regard to the assets of the common debtor (Art. 15 (1) Bankruptcy Act).

In the context of disposal over tokens, the prerequisite of power of disposal seems to be unproblematic insofar as only the holder of the Private Key has the power of disposal over the token and can thus trigger the effects of disposal. If the holder of the Private 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. If a third party has tokens, the right of disposal is effective when the person entitled to dispose of them subsequently approves it. 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 Private 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 prerequisite for a legally valid transfer of ownership rights or the establishment of limited rights in rem is the so-called agreement in rem between the seller and the purchaser. The legal concept of agreement in rem mainly serves to distinguish the transfer of ownership or the creation of rights in rem, as a transaction involving rights of disposal, from other forms of transfer (e.g. in the context of a lease or loan of use); it also makes possible a clear construct for the transfer of tokens that do not yet exist (anticipated agreement in rem). The declarations of intent underlying an agreement in rem are limited to the bringing about of the effects of the disposal (a transfer or encumbrance of ownership), the subject matter of the disposal, and the parties to the disposal transaction (minimum consensus under the law of disposal).

If one starts from the legal concept of the agreement in rem, then according to the usual rules, the point of irrevocability takes place with the exchange of the two declarations of intent; a special regulation for irrevocability in accordance with the legal rules of issuing directives does not appear necessary for this. However, the time of finality needs to be regulated, at least if TT applications are to be used for financial market transactions. “Finality” means the legal validity of a transfer transaction which has been entered on a system but was not yet executed at the time when bankruptcy proceedings were initiated. The solution proposed here corresponds to Article 3 of the EU Settlement Finality Directive.

If the disposer does not have the right of disposal, then the required condition for the lawful receipt of a token is missing. This is particularly unfortunate if the first acquirer then goes on to transfer the token to someone else, because in this case, too, the necessary authorization for disposal is missing. As a corrective, the existing property law systems therefore provide that a lack of right of disposal can be remedied under certain conditions, provided that the recipient had acted in good faith with regard to the right of disposal over the disposing party. In this case, the recipient takes over the right to dispose of the token by virtue of his/her own good faith. However, this special protection of the recipient who acts in good faith only applies if the transferee has concluded an equivalent reciprocal transaction with the transferor. Gifts or inadvertently finding a Private Key are not subject to this protection.

The conditions applicable to a good-faith purchase differ depending on the asset or property item. For example, a good-faith purchase of movables is possible only if the owner entrusted the property item to the person exercising disposition, however, not if this person loses it. On a TT System this can essentially happen as the result of losing the Private Key on a smartphone or in a hardware wallet. Under immovable property law, a good-faith purchase is linked to entry in the land register. Since the technology of TT Systems also fulfils a registration function and is characterised by a high degree of reliability, it is logical to follow the principle of the entry in the register here as well and also enable the good-faith purchase of lost property items.

This function could be made possible by registering Public Keys, e.g. with a TT Identity Service Provider. In this case, the allocation of the Public Key to the owner would simplify proving the loss or theft of a Private Key.

It should be borne in mind that a good-faith purchase is generally only able to cure the absence of the right of disposal, but it does not attach when the right of disposal is lost or lapses for other reasons, e.g. as the result of the levy of distraint, initiation of bankruptcy proceedings or a lack of legal capacity.

The disposal transaction also requires two further preconditions: the transfer of the tokens in accordance with the rules of the TT system, and the agreement of the parties that the right of disposal is to be transferred to the recipient or that a lien or usufruct is to be established on the token. A detailed regulation of the transfer process is hardly possible today if one wishes to avoid the risk that the regulations will quickly become obsolete or even prove to be an obstacle to future technological development; so here, too, one can just refer to the rules of the system. Such a reference to the rules of the system also allows for the possibility of establishing ownership-free rights in rem to a token, for example, by means of control agreements or “earmarking”.

Disposal is not granted without a legal reason, usually it is done to fulfil a corresponding obligation under the law of obligations (a transaction that imposes a legal obligation). This may be, for example, a purchase contract or a hedging transaction. The transaction that imposes a legal obligation is subject to the general limits of validity under the law of obligations (illegality, immorality, violation of personal rights, etc.); it can also be contested due to lack of intent (error, deception, justified fear). Here the relationship between the obligation transaction and disposal transaction can either be regulated in such a way that the disposal does not have any effect without a valid underlying transaction (principle of causality, which applies, for example, in Swiss moveable goods and real estate law and in Austrian Law), or that the disposal also has an effect without a valid underlying transaction (principle of abstraction, which is used in the German Civil Code).

One should not overestimate the practical significance of the two systems. If the underlying transaction is invalid, the effect on disposal cannot hold up definitively in either of the two cases. If the principle of abstraction applies, compensation is based on principles of enrichment law, while the principle of causality treats the disposal as if compensation had not been made. The differences between the principles of causality and abstraction are further qualified by the fact that grounds of invalidity can cover both the obligation transaction and the disposal transaction (so-called error identity). The difference is particularly important in the case of bankruptcy of the acquirer, because under the abstraction principle the disposer without an underlying justification will only have a claim against the bankrupt’s estate under enrichment law, and so the disposer bears the insolvency risk of the acquirer.

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 circumstances documented on the IT system. This does not mean that disposition is final and absolute but rather 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 exercising unfounded disposition (or is possibly forced to do so by virtue of a court judgement).

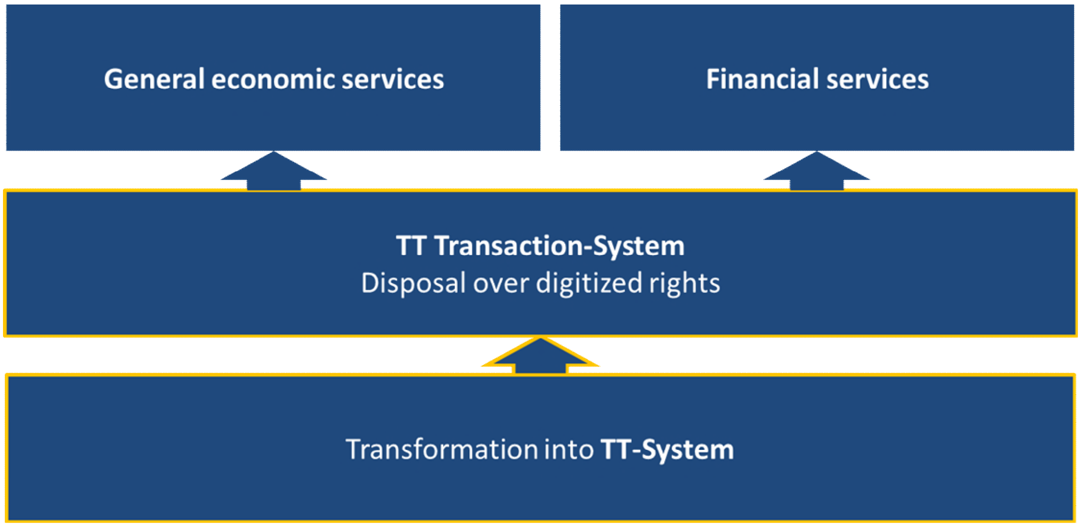
It should be noted that the Law can only regulate the right to dispose of and transfer the token. The effects that a transfer of tokens has on jurisdiction for the represented rights are only covered by Liechtenstein Law insofar as they are subject to Liechtenstein Law under the rules of Private International Law (IPRG, PRG). 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). The transfer of claims is governed by Liechtenstein Law if the third-party debtor has his/her registered office or domicile in Liechtenstein. An IP right is governed by Liechtenstein Law if it is registered in a Liechtenstein register.

Even tokens that do not embody rights will require rules about their legally binding disposal. In this context it is clear that the rules on disposal over 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.


General economic services
Financial services
TT Transaction-System
Disposal over digitized rights
Transformation into TT-System

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 embodiment 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 embodiment of the right, and the rules governing how a token can be transmitted, must be correctly represented in legal terms.

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 Issuance”.

Although the government recognises the importance of the role of the “Token Generator” in setting up a token economy, it also recognises that there are some applications in a token economy where token generation is not particularly important for protection of the user. For this reason, it has opted for a liberal regulation and created an option for token generators to register voluntarily in Liechtenstein. Token generators who value government registration and a higher level of trust of customers in their services should thus subject themselves to the Law so as to provide a kind of “quality label”. This is particularly 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 an embodiment 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 embodied 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) Avoidance of a conflict of rights: the main issue here is that the object of value is not encumbered "offline", e.g. by liens.

The Physical Validator must also contractually regulate the duties of the warehouse, i.e. so that no one may have access to the object of value without the permission of the Physical Validator. Only the person authorised to dispose of the token with the "legal title" may remove the diamond from the warehouse with the consent of the Physical Validator, provided all the associated tokens have first been cleared. This also protects the rights of all other token holders who have acquired rights to the object of value.

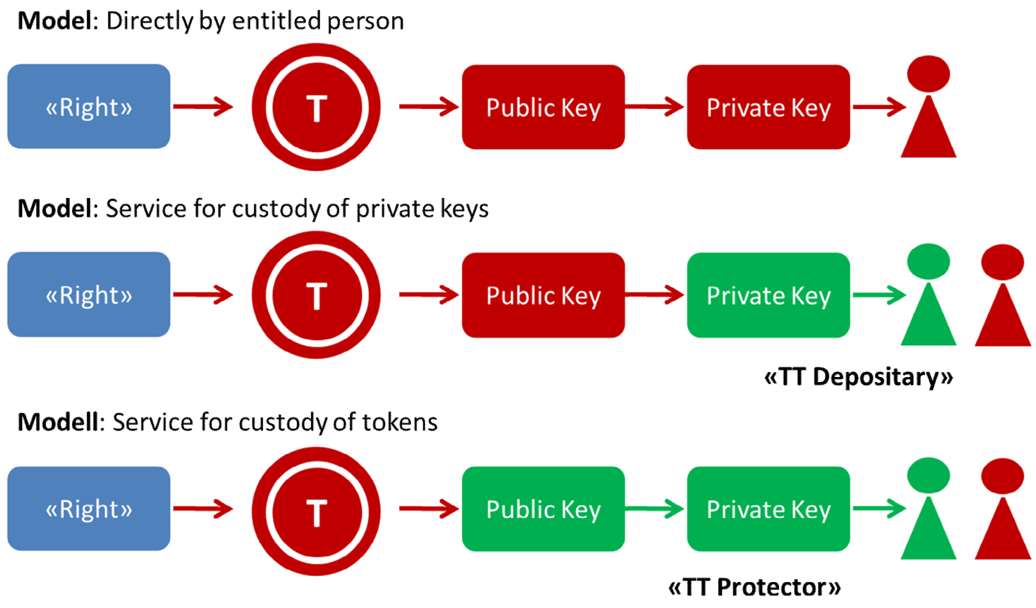
The contract between the Physical Validator and the warehouse must also stipulate that no further rights to the object may be established without the agreement of the Physical Validator. In particular, further liens may only be created via the respective Physical Validator.

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 acquire ownership of the watch if certain contractual conditions are not complied with. The question now arises, for the liquidity provider, as to whether the watch will really be available should he/she have to redeem his/her right. 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 redeem 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


Model: Directly by entitled person
«Right»
T
Public Key
Private Key
Model: Service for custody of private keys
«Right»
T
Public Key
Private Key
«TT Depositary»
Modell: Service for custody of tokens
«Right»
T
Public Key
Private Key
«TT Protector»

As described above, tokens on TT systems are always allocated to an address, the so-called "Public Key". All the tokens that are allocated to a "Public Key" can be disposed of via the "Private Key". This also means that the loss of the Private Key has major consequences, in that either the tokens are no longer available to anyone ("ownerless property") or a thief can steal the tokens, for example, by transferring them to another "Public Key". It should be borne in mind here that Private 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 Private Keys or the decedent's Private 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 Private 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 case, the Private Key is entrusted to a service provider for secure storage; in the second case, it is the token that is entrusted to the service provider.

Role of the TT Depositary

The TT Depositary keeps Private 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 Depositary will in most cases generate the Private Key directly for the customer, otherwise he/she cannot exclude the possibility that there may be several copies of the same Private Key in circulation. Typical examples are:

a) Wallet providers that store the Private Key centrally on a server, thereby reducing the risk entailed by a possible loss of the smartphone.

b) “Offline storage providers” who store Private Keys separate from the Internet in order to reduce the risk of hacker attacks.

c) “Crypto-exchanges”, which initiate the disposal over the tokens directly on behalf of the client via the Private Key, allowing trading transactions to be carried out more efficiently.

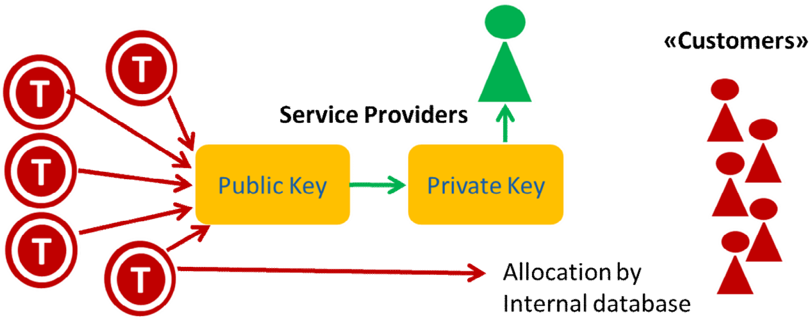
From the user's point of view, delegation leads to a risk of losing the token, especially in the case of bankruptcy of the service provider, or if the technical precautions are not sufficiently robust. With this Law the government protects the user by requiring that the tokens allocated to the Private Keys must by law be kept separate from the assets of the TT 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 Depositaries, which also takes into account their internal procedures. This is to strengthen user confidence in TT Depositaries.

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 Protector

The action of holding tokens in trust for customers in one's own name is subsumed under the role of the TT Protector. The TT Protector 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 Protector assigns the tokens of all its customers to one or more Public Keys which are in its possession and control. The allocation to the customer is done in a – usually separate – database.



Another application case for the role of the TT Protector is the protection of the privacy of customers. The TT systems known today have a public transaction log (general ledger) in which all transactions can be traced. Transactions are executed using the Public Key, which means that a transferor must know the transferee's Public Key in order to trigger a transaction. In most TT systems, this also means that the transferor can see all the tokens and transactions of the Public Key. This may be acceptable in some applications, but in terms of the full breadth of applications in the token economy it is unacceptable to a number of potential users because privacy cannot be respected at all.

To exploit the full potential of the token economy, there has to be a way to ensure protection of privacy on TT systems. By storing tokens in his/her own name, the TT Protector can help protect privacy. He/she acts outwardly as the person authorised to dispose of the tokens, and regulates the allocation to the customer via an internal database.

The government is aware that this service, besides providing a legitimate protection of privacy on TT systems, also entails the risk that it could be used for money laundering. Therefore, to minimise this risk, only service providers licensed under the Banking Act or PTA (Professional Trustees and Fiduciaries Act) are permitted to perform the role of TT Protector in Liechtenstein.

3.2.3 Token Issuance

The Law deliberately makes a distinction between the generation and the issuance of tokens, even though in today's applications in the form of Initial Coin Offerings (ICO) and Token Generating Events (TGE), 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 embodiment 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 publicly. 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 Issuance therefore concerns the initial public offering of tokens and is independent of whether the tokens were generated during or before the issuance, and whether the issuance 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 who are not personally known to the person, also features in the special protection of purchasers by the TT-Act. The processing of an issuance, 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 issuance of tokens:

Firstly, the process of token issuance in Liechtenstein will be subject to registration under the TT-Act. 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 Issuance.

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 Section II. D (Art. 28 ff.), 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 Issuance as well as the associated opportunities and risks.

The systematic structure of Art. 28-35 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 Art. 28 ff.

The main difference between a securities prospectus under the WPPG, and basic information under the TT-Act, 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, no formal approval of the information by the FMA is required.

Another important difference between the WPPG and the basic information under the TT-Act is that buyers of tokens are not necessarily investors who buy tokens primarily for the yield they can obtain. Because tokens can embody all kinds of rights, the formulations in Art. 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. For most of these ICOs, publication of basic information makes sense 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. Nonetheless, it wants to formulate the exemption provisions in an open manner, to allow for the many applications that require the legal certainty of this Law but would be made impossible by excessive regulation. 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 TT-Act 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 Issuance 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 TT-Act. There are some, however, which are particularly sensitive – just as we find on the financial market – and should be officially registered by the FMA in order to create user confidence and prevent abuse.

Such a service is, for example, an exchange, i.e. an organised market in which a large 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 TT-Act via the roles of the TT Depositary and the TT Protector. So at present there is no need for additional regulation of this aspect by the TT-Act.

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 Office Operator

Via TT Exchange Offices, legal tender such as euros or Swiss francs are transferred to TT systems. Generally, tokens are transferred that can embody all types of rights. For example, legal tender, crypto-currency, and also rights to other assets.

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 the legitimate owner of the machine is. This functionality can, for example, be applied to car-sharing companies, where a user pays for the service directly via the Public Key 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. To allow specialised service providers to develop, the government has decided to offer them the option of registering voluntarily.

3.3 Regulatory approach

3.3.1 General

When regulating TT systems, the basic question arises as to whether the technology can or should be regulated. Due to the high pace of innovation of TT systems, and the lack of an intermediary, it makes no sense for the government to regulate the technology itself. It is more effective to regulate TT Service Providers and to oblige them to critically inspect the TT systems on which they offer their services. This also implies an important advisory service that a TT Service Provider must provide in order to offer its customers the necessary legal certainty. Moreover, in this way service providers can respond quickly to the various developments on TT systems (e.g. forks[7]).

As explained in Section 2.2, 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 2.2 also explains that there are new application scenarios on TT systems regarding money laundering and criminal abuse.

With the TT-Act, 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 reputation of the country. TT Service Providers must register with the Financial Market Authority (FMA).

These requirements and the obligation to register apply only to service providers domiciled in Liechtenstein, and not to companies or private individuals domiciled abroad who offer TT services to residents of Liechtenstein. This is because, firstly,

[7] 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 Etherium blockchain, so that two TT systems are now continued as Ethereum and Ethereum Classic.

it would not be feasible in practice to control such services offered over the Internet. Secondly, the chosen approach also allows Liechtenstein residents to take personal responsibility in deciding whether they choose a regulated or an unregulated service provider.

The government is aware that by imposing the legal requirements for TT Service Providers it is creating a certain hurdle that does not exist in other countries in this form. Nevertheless, it is confident that on the whole it is attractive for TT Service Providers to register in Liechtenstein, because these minimum requirements can also represent a quality label for the companies, and thus a sales argument, vis-à-vis their customers. What is more, TT Service Providers receive greater legal certainty than in other jurisdictions.

However, for the TT Service Providers the time it takes before they can start their business activities is of the utmost importance. Therefore the government will not require an extensive state audit of the companies, such as we usually find in the financial market, and instead is introducing a less time-consuming registration procedure. This registration procedure makes it possible to check the reliability of a TT Service Provider, to obtain an overall view of all active TT Service Providers in Liechtenstein, and with the option to withdraw the licence of a TT Service Provider if the legal requirements are not met.

However, a deliberate decision was made not to check the professional qualifications, because no training standards have been established in this sector at the present time. A well-founded review of the professional qualifications by a government office would lead to a disproportionate outlay.

For the time being, the government has also decided not to introduce an ongoing prudential supervision of TT Service Providers, because this would involve a great deal of work on the part of the companies and the FMA, and at present there is no body of experience to refer to concerning the need or effectiveness of such measures.

The government and the FMA 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 TT Service Providers are explicitly not subject to the financial market legislation, the government is of the opinion that the Financial Market Authority is the authority best suited to this task. Today, apart from the Ministry for General Government Affairs and Finance, only the "regulatory laboratory" of the FMA has in-depth experience with IT 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.

A legal definition of the minimum requirements for TT Service Providers is necessary, not only to protect users and the country's reputation; the government believes that the token economy can only develop to the full if users have very firm confidence in the service providers who are involved in the transformation of the "real" world onto TT systems or who provide the basic services.

The government requirements and registration, therefore, also correspond to a strong wish on the part of the companies that want to provide services on TT systems.

This wish for a government "quality label" is not only entertained by TT Service Providers, who are obliged to register in the interests of the state to protect their customers and reputation, but also by other service providers that are important in a token economy, such as Token Generators, TT Verifying Authorities and TT Price Service Providers. User confidence in these service providers is particularly important to ensure the efficiency of TT systems. The government would like to offer these service providers the option to voluntarily comply with the state minimum requirements, and in return allow them to register in the TT Service Provider Register.

However, some configurations are also conceivable in which the state minimum requirements are not appropriate. In view of this, the government does not wish to restrict the innovative power of the token economy and refers to voluntary registration.

To do justice to business model innovation, the various activities on the TT systems are formulated in terms of functionality and can thus be put together individually in a modular way in order to achieve a “bespoke” regulation.

3.3.2 Procedure

The fourth section of the TT-Act contains provisions on the registration of TT Service Providers. This section was modelled on international models, such as the registration procedure under §§ 339 et seqq. Austrian Trade Regulations Act, §§ 14 et seq. German Trade Regulations Act and the registration procedure for account information service providers under the future Liechtenstein Payment Services Act (Art. 12).

Unlike licensing procedures under the relevant financial market laws, TT Service Providers are only subject to a limited review procedure, which is concluded with an entry in the Service Provider Register (Art. 37 and 41). And unlike financial intermediaries, TT Service Providers do not, for example, have to check the owners (there is no monitoring of shareholdings); nor is there a detailed analysis of the equity structure of the service provider. There is also no inspection of the organisational requirements that TT Service Providers have to meet, unlike the situation with banks and securities firms. Due to the reduced risk for customers as a result of a bankruptcy, the capital requirements for TT Service Providers are set at the level of asset managers in accordance with the Asset Management Act (VVG).

Registration (entry in the TT Service Provider Register as indicated in Art. 41) is constitutive and establishes the subjective right of the TT Service Providers referred to in Art. 36 (1) to provide their services in Liechtenstein. Appropriate applications for registration may be submitted to the FMA by individuals as well as legal entities.

For the purposes of this Law, the FMA must examine whether a TT Service Provider is capable of acting and is reliable, and whether the required capital or equivalent securities are available. Due to the novelty of TT systems, an examination by the FMA as to whether TT Service Providers are technically suitable to carry out the activities can hardly be implemented in practice. For this reason, the government has decided not to carry out a state examination of professional qualifications in order not to impede innovative capability.

Nonetheless, the way in which the requirements for personal qualifications and internal procedures are formulated does mean that TT Service Providers are required to use state-of-the-art procedures.

Should there be any indications that the legal requirements are not being complied with, the FMA may prohibit a TT Service Provider from carrying out its activities.

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 (SPG). Developments in recent years in the area of FinTech, especially virtual currencies, have opened up new questions, and these have already been addressed in the 4th Money Laundering Directive (exchange of official tender to virtual currencies in a currency exchange office).

Exchange Offices within the meaning of Art. 3 (1) lit. f SPG must therefore exercise the due diligence obligations under the SPG when they exchange virtual currencies for legal tender, and vice versa, in the amount of CHF 1,000 or more. According to Art. 2 (1) lit. l 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.

Considering the wide range of possible applications of TT systems, the question arises as to how virtual currencies are to be defined and differentiated from other tokens.

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

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, which go beyond the current international and European standards.

The government is therefore extending the scope of the SPG to cover the relevant activities on TT systems:

Exchange Office

The current definition of the currency exchange office in the SPG refers only to virtual currencies. Considering the much larger assets that can be exchanged directly via tokens and thus transferred to TT systems, the definition of the currency exchange office is to be extended to cover general tokens. In addition, the exchange between tokens, for example between two cryptocurrencies, is also covered.

Token Issuer

The issuing of tokens is also a possible entranceway for assets entering into Liechtenstein. To avoid misuse, the Token Issuer is also placed under the scope of the SPG.

TT Protector

The TT Protector, because of the fiduciary safekeeping of tokens for customers, is of central importance from the viewpoint of money laundering. For this reason, the exercise of an activity as a TT Protector today requires a licence in accordance with the Banking Act and the Professional Trustees and Fiduciaries Act (PTA), which means that they are already subject to the SPG.

Physical Validator

Physical Validators, as the interface between physical objects and the TT system, play an important role in the integration into the TT system and should be subject to due diligence.

TT Depositary

Even if a TT Depositary only keeps Private 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.

TT Identity Service Provider

To facilitate the possible delegation of the task of identifying contracting parties on TT systems, TT Identity Service Providers will also be subject to the SPG.

3.5 Uncertificated rights

The issuing of securities by Liechtenstein companies will be an important application in TT systems. The Liechtenstein Persons and Companies Act (PGR) defines a security as “a document in which a right is certificated in such a way that it cannot be used, asserted or transferred to others without the document” (§ 73 Final Section PGR). For securities to be embodied in a token on a TT system, and transferred there, via a physical document without any detours, the legal concept of the book-entry security (*Wertrecht*) has been introduced into Liechtenstein Law, and at the same time the interface between securities law and the TT-Act is created. Uncertificated rights are dematerialised securities in which the document is replaced by the so-called register of uncertificated rights or book-entry register. The entry in the uncertificated rights register is constitutive both for the creation of book-entry rights and for their transfer. TT Systems are perfectly suited for issuing and transferring uncertificated rights 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. § 81a Final Section PGR is based on Art. 973c of the Swiss Code of Obligations, but goes further than that on various points, specifically to allow legal certainty for interfaces to TT applications.

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. This Law is not contemplated to govern the TT Services offered by foreign providers that are used by persons resident in Liechtenstein.

TT Service Providers domiciled in Liechtenstein who may voluntarily register are therefore subject to this Law only if they have registered or if they have explicitly declared the Law, in particular the provisions pertaining to the right of disposal over tokens and the disposition over tokens pursuant to Chapter II, to be applicable to them.

The same applies to tokens that have been generated by a company domiciled outside of Liechtenstein. The purpose of this liberal regulation is to create legal certainty in the global token-based economy given that no corresponding provisions are currently known to exist.

The TT-Act 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.

4. ARTICLE-BY-ARTICLE COMMENTARY

Re: Art. 1

The purpose of this Law is to protect users on TT Systems and to secure their trust in digital rights. Trust in digital rights arises primarily by creating a body of "property law" for digital property located on TT Systems (Chapter II). No significant legal certainty can be ensured for users on TT Systems until this has taken place. In so doing, the user is protected when he/she purchases tokens and rights embodied in tokens. This also means that these rights can be enforced under the law. This protection is of fundamental importance not only for users but also for all professional service providers on TT Systems.

Another key aspect of user protection is clarity pertaining to the treatment of Private Keys and tokens that are transferred to professional service providers when powers of disposal are delegated in the event of bankruptcy.

A third aspect of user protection pertains to ensuring a minimum level of quality of TT Service Providers. This notion of protection is also a central component of other commercial legislation and is based on the principle that users are structurally inferior to the service providers, meaning they may be at a disadvantage as a result of a lack of expertise, information, resources and/or experience. The concern and task of user protection is to judiciously redress this imbalance and to aid in appropriately advancing consumer interests in interactions with providers.

The TT-Act also implicitly provides for protection of the TT Service Providers. Given the many possibilities that are afforded to TT Service Providers by this new technology, there are many unresolved issues relating to the application of law and delimitation with respect to other laws. Consequently, it also caters for a substantial need of the market for clarity. Therefore the purpose of the TT-Act is to also provide for the protection of service providers by creating legal certainty.

This Law also governs the registration and supervision of service providers that provide services on TT Systems. The rights and obligations of service providers are also established.

Re: Art. 2

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. This Law is not contemplated to govern the TT Services offered by foreign providers that are used by persons resident in Liechtenstein.

TT Service Providers domiciled in Liechtenstein who may voluntarily register are therefore subject to this Law only if they have registered or if they have explicitly declared the Law, in particular the provisions pertaining to the right of disposal over tokens and the disposition over tokens pursuant to Chapter II, to be applicable to them.

The same applies to tokens that have been generated by a company domiciled outside of Liechtenstein. The purpose of this liberal regulation is to create legal certainty in the global token-based economy given that no corresponding provisions are currently known to exist.

Paragraph 3 establishes that the TT-Act is designed to close any gaps that have arisen to date as a result of the new technologies. Where other statutes are applicable to a service on a TT System, the provisions of these statutes remain in full force and effect. If, for example, banking or securities services are offered on a TT System, the provisions of the Banking Law (BankG) or the Asset Management Law (VVG) apply.

Re: Art. 3

Article 3 sets out the requirements that must be satisfied by trustworthy technologies. Here tokens assume a central role as containers embodying a right on a TT System. Users are able to have assets show on TT Systems or to purchase them only if it is reliably ensured that the tokens are unique and tamper-proof. Under no circumstances may tokens be copied or altered. "Integrity" is an information security concept that usually refers to the accuracy and consistency of data over its entire lifecycle. It encompasses these key requirements to be satisfied by tokens.

Another central element of TT Systems is the unambiguous allocation of tokens to the owner who possesses the power of disposal over them. Systems that do not provide for this unambiguousness and protection against tampering by unauthorised persons are not trustworthy. No one except for the owner may have the power of disposal over the tokens and be able to transfer them to another person, for example.

These requirements categorically apply to all transaction systems regardless of whether or not they employ trustworthy technologies. However, the special feature of TT Systems is the absence of an operator who guarantees the quality and integrity of the transaction system. In TT Systems, trustworthiness arises by virtue of the technology itself that ensures the integrity of the tokens and the trade repository through encryption technology, the principle of distributed ledgers, predefined rules, etc. That is why the term "trustworthy technologies" refers to technologies that are trustworthy per se without an operator being responsible for them. Paragraphs 1 and 2 summarise these requirements and features in as technology-neutral a manner as possible.

Owing to the breakneck pace of innovation of the underlying technologies, it would not be useful to establish more concrete legal descriptions that are in reference to a specific embodiment of current technologies, since this might quickly give rise to delimitation issues and, as a consequence, legal uncertainty.

Re: Art. 4

This provision sets out, in a manner similar to other supervisory statutes (cf., for example, Art. 3 Payment Services Act (ZDG); Art. 3 Business Act (GewG)), exceptions from the personal scope of application of the TT-Act.

Whereas the first exception (central banks, national and municipal authorities) is self-explanatory, the term “closed user group” (sub-para. b) is defined as services that are provided by way of private systems and technologies and are consequently not accessible by the general public and – as a rule – are not provided commercially, and are therefore to be exempted from the TT-Act (e.g. issue of tokens within a group of companies, exchange of tokens and crypto-currencies among friends and acquaintances, supply chain management of an industrial firm).

Re: Art. 5

The purpose of Art. 5 is to define key terms and concepts that are used in part with different meanings in everyday speech. It should be borne in mind that some terms are defined specifically as they relate to and are used in this Law. This is noted specifically in the respective comment.

Para. 1 item 1 “Token”

Para. 1 item 1 defines the concept of a “token”. “Token” is borrowed from English, and, as such, has multiple meanings in everyday use. It also has various meanings in relation to blockchain technologies. This makes it all the more important to introduce a legal definition of “token”. A token represents a piece of information on the TT system. In the case of Bitcoin, it is the information indicating what amount of Bitcoin is allocated to which Public Key.

In Report and Motion no. (BuA) 2016/159,[8] Bitcoin is listed as an example of a virtual currency. There “virtual currency” is understood to be “digital monetary units” that do not officially qualify as legal tender, which, however, can be exchanged for legal tender for the purpose of purchasing goods or services or used as a store of value and, in so doing, assume the function of legal tender. From a regulatory perspective, it is currently common in some cases[9] to classify tokens as utility tokens, payment tokens (currency coin), and security tokens (equities; assets).

The government has purposely not undertaken to classify tokens because, apart from being used as a means of payment, under this Law “token” is also construed to be a “container”[10] that may serve as a vehicle for any type of justified claims or membership rights vis-à-vis a person, rights in property or other absolute or relative rights. Therefore, which *lex specialis* provisions are applicable must be examined in keeping with the specific form a token takes; hence the government is of the opinion that classification would result in improper simplification.

[8] Report and Motion of the Government to the Parliament of the Principality of Liechtenstein concerning the amendment of the Due Diligence Act (SPG) and other laws.

[9] See FINMA Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs), published on 16 February 2018.

[10] Container.

Consequently, apart from this Law, and depending on the concrete form a token takes, the applicability of other *lex specialis* provisions – in particular those set out in Art. 5 of the Financial Market Supervision Act (FMAG) – must be examined.

Para. 1 point 2 "Public Key"

Para. 1 item 2 defines "Public Key". "Public key" as used in this draft bill refers to a sequence of characters (e.g. 1LQrs2zJRD9ASfLxaBSiS1iUhfrcJJPDns).

This term is used in asymmetric cryptography or public-key cryptography that represent encryption schemes. A pair of keys (consisting of a Private Key and a Public Key) enable users to exchange encrypted information without having to exchange a common key beforehand. "Public key" is used here as shorthand to refer to the "public" component of any asymmetric cryptography solution.

The government is cognisant of the fact that "Public Key" may be in reference to one possible embodiment of TT Systems, but has dispensed with coining a new term for the sake of clarity. Yet this term is to be viewed strictly in legal functional terms.

Para. 1 item 3 "Private Key"

Para. 1 item 3 defines "Private Key". This term is also used in asymmetric cryptography or public-key encryption schemes. The Private Key enables the individual who possesses the power of disposal to decrypt data that has been encrypted using the Public Key, as well as to generate digital signatures and thus carry out transactions. "Private Key" is used here as shorthand to refer to the "private" component of any asymmetric cryptography solution.

Para. 1 item 4 “Users”

Para. 1 item 4 defines “users” as persons who use TT Services. This term is purposely broader than “consumer” or “investor” because the latter only reflect part of the possible applications of a token-based economy.

Para. 1 item 5 “Issuing of Tokens”

Para. 1 item 5 defines “issuing of tokens” as an offering to the public in any form and by any manner of notification for the purpose of selling tokens to users. The issuing of tokens is generally known under the name of ICO (Initial Coin Offering) or TGE (Token Generating Event).

Para. 1 item 6 “Basic Information”

Para. 1 item 6 defines “basic information”. White papers generally satisfy a similar function in relation to ICOs.

Para. 1 item 7 “TT Service Provider”

Para. 1 item 7 defines “TT Service Provider” as a person who engages in one or more activities in accordance with points 8–16.

Para. 1 item 8 “Token Issuer”

Para. 1 item 8 defines “Token Issuer” as a natural or legal person who engages in the issuing of tokens. This can take place in the issuer’s own name (self-issued), or on behalf of a third party.

Para. 1 item 9 “Token Generator”

Para. 1 item 9 defines “Token Generator” as a service provider who engages in giving tokens a concrete form. The service provider creates rules (software) determining how the tokens behave, which interactions are possible, and, in particular, the conditions under which tokens may be transferred. Tokens can accordingly be created on existing TT Systems (e.g. ERC20 tokens on the Ethereum blockchain), or on one’s own TT Systems. Thereby the Token Generator need not develop a TT System of their own.

Para. 1 item 10 “TT Depositary”

Para. 1 item 10 defines “TT Depositary” as a service provider who holds Private Keys for beneficial owners in safekeeping. It is the legislator’s objective to subject the safekeeping of Private Keys to specific requirements or safeguarding measures. “TT Depositary” must be distinguished from the term “custodianship” used in the Banking Act (BankG) since no management services are provided by the TT Depositary. Consequently, it is possible for the TT Depositary to safekeep the Private Keys of tokens that represent financial instruments.

Para. 1 item 11 “Physical Validator”

Para. 1 item 11 defines “Physical Validator” as a service provider who creates the link between a token and the right to a property item that is embodied in the token and ensures the enforcement of the rights embodied in the token. Therefore the idea is that a customer approaches a Token Generator with an order to tokenise rights in an asset or property item (e.g. a watch) owned by the customer by issuing a token embodying the rights to this item.

Para. 1 item 12 “TT Protector”

Para. 1 item 12 defines “TT Protector” as a service provider who provides typical fiduciary services relating to a TT System to protect the privacy of users. TT Protectors act in their own name or on behalf of one or more third parties.

Para. 1 item 13 “TT Exchange Office Operator”

Para. 1 item 13 defines “TT Exchange Office Operator” as a service provider that discloses the current market prices of tokens and exchanges tokens against legal tender or vice versa. This includes Bitcoin machines (also Bitcoin ATMs) and crypto-exchanges.

Para. 1 item 14 “TT Verifying Authority”

Para. 1 item 14 defines “TT Verifying Authority” as a service provider who ensures that in their disposition over a token the contracting parties possess legal capacity and that any other purchase or transfer conditions are complied with as applicable. This can also be performed by a software.

Para. 1 item 15 “TT Price Service Provider”

Para. 1 item 15 defines “TT Price Service Provider” as a service provider whose main task is to publish current aggregated price information on tokens.

Para. 1 item 16 “TT Identity Service Provider”

Para. 1 point 16 defines “TT Identity Service Provider” as a person who identifies the individual authorised to dispose of a Public Key and records them in a directory.

Para. 1 item 17 “TT Systems”

Para. 1 item 17 defines TT Systems as transaction systems that ensure the secure exchange and storage of digital representations of rights, as well as the provision of services based on them, by way of trustworthy technologies in accordance with Art. 3. “Transaction system” constitutes an overarching concept that covers all conceivable processes involving tokens in order to symbolise the extremely broad scope of a token-based economy. This includes trading activities, exchanges, transfer of rights in general, to name only a few. “Secure exchange and storage” are to be understood as general quality criteria without which a TT System cannot be trustworthy. The criterion of secure storage refers in particular to the digital representation of rights and their integrity, not to the safekeeping of the Private Keys.

Re: Art. 6

Para. 1: The person possessing the right of disposal is the holder of the full legal title to a token, i.e. this person may legally dispose of the token and is deemed the owner of the right embodied in the token. According to the current state of knowledge, however, disposal over tokens cannot be exercised directly, but only by way of the Private Key. This means that a duality exists in the right of disposal over a token and over a Private Key. This is why the right of disposal under this Law is linked to a Private Key.

Disposal over a Private Key can be gained de facto by way of the tokens allocated to the associated Public Key. Therefore the holder of the Private Key has the power of disposal over the token. Yet the holder need not be the person possessing the right of disposal. If a Private Key is stolen, the thief 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.

In order for application to TT Systems to be practicable, the Law proceeds from the assumption that the holder of the power of disposal is also the person possessing the right of disposal. This means that if the thief gains the power of disposal over the Private Key, it is presumed that he/she is also the person who is authorised to dispose of it. However, this legal presumption is rebuttable. A rebuttable legal presumption reverses the burden of proof, meaning the victim of the theft bears the onus of proving that he/she is the rightful owner, i.e. the lawful person possessing the right of disposal. The lawful person possessing the right of disposal is whoever can demonstrably show that they received the token by way of transfer from a person possessing the right of disposal or that they originally purchased the token.

This provision is applicable in substance to the situation, occurring frequently in practice, that disposal over a token can be effected only by way of multiple Private Keys (multi-signature).

Para. 2: Art. 7–12 encompass provisions relating to the disposition over tokens which, on the whole, are of central importance primarily for tokens with embodied rights. For the special case of "empty" tokens, i.e. tokens in which no rights are embodied (e.g. fiat crypto-currency), the application of Art. 7 and 9 pertaining to the effect of disposition on the embodied right and the proof of authorisation on the part of the person possessing the right of disposal does not make any sense. This paragraph aims to establish that the provisions of Art. 8, 10, 11 and 12 also apply to empty tokens in order to ensure the requisite legal certainty.

Re: Art. 7

Para. 1: As explained in Chapter 3, generating a token does not cause a new right to be created but rather causes an existing right to be subjected to the transfer and proof of authorisation rules of the TT System. If the token is filled, the right now embodied in the token is transferred in accordance with the rules of the TT System (transfer rules). By embodying a right in a token, the transfer of the token equates to the transfer of the right embodied in the token, provided that transfer is lawful and contractually permissible. Upon the transfer of the token, the transferee (recipient) becomes the person possessing the right of disposal and thus also automatically the lawful owner of the right embodied in the token or the owner of the property embodied in the token.

Para. 2: In order to guarantee the correct functioning of a TT System, a direct link must be ensured between a right on the TT System and the embodied right.

Consequently, the Token Generator has the obligation of ensuring, by way of suitable measures, that disposition over the token actually results in direct disposition over the embodied right and that any other disposition over the right embodied in the token is precluded. The other obligations of a Token Generator are set out in further detail in Article 19.

Para. 3: This paragraph aims to establish that transfer of disposition also includes the transfer of the right of disposal over the token.

Re: Art. 8

As previously set out in Chapter 3, three elements need to be satisfied in order to bring about lawful disposition:

a) Completion of disposition in accordance with the rules of the system:

   Providing detailed stipulations for the transfer process per se is virtually impossible today if one does not want to run the risk of the stipulations quickly becoming obsolete or their even proving an obstacle for future technological development; consequently, there is no other choice here but to make reference to the rules of the system. Making reference to the rules of the system leaves the possibility open of establishing non-possessory rights in rem in tokens, e.g. by way of control agreements or earmarking.

b) A declaration made by the transferor and the transferee:

   The requirement for the legally valid transfer of title or the establishment of restricted rights in rem is an in rem agreement between the transferor and transferee.

   The declarations of intent on which the in rem agreement is based are limited to bringing about the effects of disposition (transfer of the right of disposal), the object of disposition and the parties to the disposition transaction (minimum consensus concerning right of disposal). No formal requirements apply to this declaration, it is also valid by implication.

c) Transferor’s right of disposal:

Disposals are not effective unless the person exercising disposal possesses the right of disposal, i.e. is authorised to initiate the change in legal status at issue. The lawful person possessing the right of disposal is whoever received the token by way of transfer from a person possessing the right of disposal or originally purchased it.

Para. 2: 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). 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 exercising unfounded disposition (or is possibly forced to do so by virtue of a court judgement).

TT Systems are generally characterised by the fact that verified transactions cannot be unwound. Deletion or cancellation as is common in other transaction systems is not possible. This is frequently the argument cited that disposition over a token must be lawful.

Therefore it is important to stipulate that only the de facto power of disposal is unambiguously transferred by way of the technology and not necessarily also the right of disposal as well. Consequently, the provisions of the General Civil Code pertaining to unjust enrichment can be applied to dispositions that are legally unfounded. Even if a transaction cannot be deleted in technological terms, the de facto power of disposal can be transferred to the lawful person possessing the right of disposal so that the lawful condition can be restored.

Para. 3: This section is intended to provide a stipulation specifying the point in time at which disposition over a token is lawful for the event of debt enforcement proceedings. Similar provisions are contained in financial market law (cf. Art. 3 of the EU Settlement Finality Directive).

Re: Art. 9

Proof of authorisation deals with the question of whom an obligor may and must recognise as being authorised in the case of claims or membership rights. “Obligor” refers to a debtor or a company, for example. The following generally applies: Only payment to a material beneficiary obligee has discharging effect; if there is any doubt concerning this, the obligor may and must refuse to effect payment. Consequently, securities law stipulates that the obligor is relieved of their obligation by way of payment to the holder of the security and that they cannot demand that the holder of the security provide any further proof of their creditor status. These “proof of authorisation rules” form central requirements for the marketability of securities and are to apply to tokens as well, also and especially since the legal title evidenced by the TT System provides for a high degree of reliability in this case.

Re: Art. 10

If the person exercising disposition lacks the right of disposal, a definitional prerequisite for the purchase of a token is lacking. This is all the more unfortunate if the initial purchaser transfers the token onward, since the requisite right of disposal is lacking in this case. This Law provides for special protection of the transferee if they acted in good faith with regard to the transferor’s right of disposal. In this case, the purchaser originally acquires legal title to the token in good faith. However, this applies only if the transferee has entered into a counter-transaction of equal value with the transferor. Gifts or inadvertently finding a Private Key are not subject to this protection.

The conditions applicable to a good-faith purchase differ depending on the asset or property item. For example, a good-faith purchase of movables is possible only if the owner entrusted the property item to the person exercising disposition, however, not if this person loses it. On a TT System this can essentially happen as the result of losing the Private Key on a smartphone or in a hardware wallet. Under immovable property law, a good-faith purchase is linked to entry in the land register. Since the technology of TT Systems also fulfils a registration function and is characterised by a high degree of reliability, it is logical to follow the principle of the entry in the register here as well and also enable the good-faith purchase of lost property items.

This function could be made possible by registering Public Keys, e.g. with a TT Identity Service Provider. In this case, the allocation of the Public Key to the owner would simplify proving the loss or theft of a Private Key.

It should be borne in mind that a good-faith purchase is generally only able to cure the absence of the right of disposal, but it does not attach when the right of disposal is lost or lapses for other reasons, e.g. as the result of the levy of distraint, initiation of bankruptcy proceedings or a lack of legal capacity.

Re: Art. 11

Art. 11 sets out the territorial scope of the provisions pertaining to the right of disposal and the persons to whom this applies. Since TT Systems do not possess a legal point of reference in relation to a specific country, it is important that the scope of application of the rules pertaining to the disposition of tokens (Art. 6–10) be defined in terms of an international context. Legal certainty for a token-based economy not only assumes a clear-cut and unambiguous allocation of ownership rights and rights of disposal, but also clarity pertaining to applicable law. In practice, this issue is frequently anything but clear because, being decentralised systems, TT Systems elude an unambiguous allocation to a specific jurisdiction.

It is obvious that these rules are in relation to the tokens themselves and not primarily the TT Service Provider, since private users must also be able to benefit from this legal certainty, irrespective of whether or not they use the services of a TT Service Provider.

Consequently, Art. 11 provides for two alternative criteria. According to sub-para. a, the provisions concerning disposition over tokens apply if the tokens are generated or issued by a TT Service Provider that is subject to Liechtenstein Law pursuant to Art. 2 of this Law. This case appears to be unproblematic in that there is an unambiguous link between the TT System and Liechtenstein and it is presumably more closely linked to Liechtenstein Law than to any other law. Sub-para. b additionally offers the possibility of a choice of governing law. In other words, the disposition rules of this Law are also to be invoked if the Token Issuer has chosen Liechtenstein Law although no TT Service Provider is domiciled in Liechtenstein. This is justified by the fact that the territorial attribution of TT Systems to a specific jurisdiction is frequently exceptionally difficult because the legal relationship has no focal point. In any event, a choice of governing law provides the possibility to create unambiguous legal relationships. The choice of governing law must be explicit; it cannot be inferred from the circumstances. Art. 11 sub-para. b does not impose any formal requirements on the choice of governing law; specifically, there is no requirement of the written form, as this would constitute a virtually insurmountable obstacle for the digital economy. Otherwise, requirements, effects and restrictions are determined by the general provisions of private international law (Art. 11, 39 et seqq. Act on International Private Law (IPRG)).

Hence the first scope of application of these provisions is specified for tokens that are generated or issued by a TT Service Provider domiciled in Liechtenstein (sub-para. a). Sub-para. b has purposely been drafted in a very open manner so that this possibility exists for other situations. In so doing, existing tokens can be subsequently voluntarily subjected to these provisions, as can tokens that are generated by the user himself or herself, or tokens that are generated or issued outside of Liechtenstein, so as to benefit from this legal certainty.

Re: Art. 12

This article is a pure jurisdiction clause. The jurisdiction of Liechtenstein courts is of significant importance because they determine the applicable law according to Art. 11, whereas foreign courts consult their own rules on conflict of laws. Consequently, the object here is not to impose Liechtenstein Law on foreign law but rather to provide for legal certainty that is as broad as possible.

This article first establishes that a token is deemed an asset located in Liechtenstein provided that the TT System is subject to Liechtenstein Law pursuant to Art. 2. In so doing, the place of jurisdiction is at the place where the property is located in terms of section 50 para. 1 of the Jurisdiction Act (JN). In addition, a fiction of law is established according to which the choice in favour of Liechtenstein Law (explicit submission pursuant to Art. 11 sub-para. b) also equates to a jurisdiction agreement in terms of section 53 Jurisdiction Act (JN). Agreements on the jurisdiction of a court are broadly recognised in international civil procedure law.

Re: Art. 13

This provision establishes general requirements with which TT Service Providers must comply pursuant to Art. 36 para. 1. These requirements (no criminal record; must be reliable; must have capacity to act) apply firstly to natural persons who seek to provide services subject to registration, and secondly to the executive management members of a legal entity (para. 2).

The requirements set out in this Law must be continuously satisfied upon registration and for the entire duration of operation as a TT Service Provider. Consequently, pursuant to Art. 41 (cf. para. 3 sub-para. a), the FMA may not enter an applicant in the TT Service Provider Register who has a criminal record and whose conviction has not been expunged.

Art. 13 paras. 1–3 establish the relevant “grounds for excluding applicants from registration”.

Paras. 1–3 have been modelled according to the functionally similar Art. 8 et seqq. Liechtenstein Trade Act (GewG) and sec. 8 et seqq. Austrian Trade Ordinance (GewO). Consequently, these provisions can also be consulted for interpreting Art. 13 paras. 1–3.

Para. 4: Notwithstanding paras. 1-3, para. 4 is to be viewed as establishing qualified organisational requirements for TT Service Providers subject to registration. These requirements (e.g. clear-cut organisational structure; procedure in place for avoiding conflicts of interests) must also be satisfied by TT Service Providers on a continuous basis and set out in a corresponding organisational document. Unlike the other paragraphs, the requirements set out in para. 4 must be satisfied by all TT Service Providers regardless of their legal form.

Where Art. 13 para. 4 sub-para. c compels TT Service Providers to maintain a sufficient amount of minimum capital or to take out “equivalent security”, this is in reference to a bank guarantee or sufficient liability cover. The amount of minimum capital depends on the asset management company and its exposure as set out in Art. 8 Asset Management Act (VVG).

Para. 5: Para. 5 establishes that TT Service Providers pursuant Art. 36 para. 2 who register voluntarily must also satisfy the requirements set out in paras. 1–4.

Re: Art. 14

Art. 14 sets out the special requirements that are applicable to Token Issuers. By definition, they perform the issuing of tokens (ICOs / TGEs) for themselves or on behalf of third parties. The government establishes that in current practice Token Issuers, apart from issuing tokens, also generate them in most cases. However, there are also already cases in which the generation of tokens is contracted out to third parties.

A Token Issuer is only whoever publicly offers one or multiple generated tokens. It is immaterial whether the Token Issuer does this for their own account or the account of third parties.

However, this Law is not intended to apply to persons who engage in direct trading of generated tokens with other parties in transactions that are not open to the public (OTC trading).

The government provides for a registration obligation for Token Issuers. Already prior to the entry into force of this Law, it is already common practice for the FMA to examine the business models underlying the issuing of tokens for activities subject to licensing.

Art. 14 sub-para. a obligates Token Issuers to disclose the basic information pursuant to Chapter III D of this Law at the time of token issue and up to ten years subsequent to completed issuance. The purpose of this is to enable users to obtain information about the tokens being publicly offered or previously publicly offered and to make an informed judgement about the rights and risks associated with the tokens as well as the service providers involved.

In light of Art. 1059 para. 1 Persons and Companies Act (PGR), it appears appropriate to the government to compel Token Issuers to retain and disclose the basic information for a period of ten years subsequent to completing the issuance of tokens. Retention and disclosure in electronic form are possible provided that the requirements pursuant to the Persons and Companies Act (PGR) and its ordinance are observed. The time at which this basic information is saved can be documented by employing a trustworthy technology contemplated by this Law.

Art. 14 sub-para. b obligates Token Issuers to execute customer orders relating to the issuing of tokens in accordance with the customer's instructions, specifically as regards volume, price, and the like.

Art. 14 sub-para. c obligates Token Issuers to ensure that a token publicly offered by them and the associated right have not been previously issued. If, for example, the title to a specific asset or item of property (a bicycle is used here for the sake of illustration) has been previously tokenised and this token has been issued, reissue is to be prevented. This is emphasised given that it is comparatively easy to create a token and to issue it.

What is not meant, for example, is if an access right to a platform is tokenised and, as a result, further tokenised access rights are issued.

The government has deliberately opted to compel Token Issuers to prevent duplicate issue by way of statute. Pursuant to Art. 20 sub-para. a, the Physical Validator also must ensure that the customer commissioning the generation of a token may lawfully dispose of the right being tokenised at the time of generation so as to prevent a conflict of rights, especially where rights in the same property item are tokenised (e.g. duplicate tokenisation of title to the same property item). In addition, the government takes the view that the Token Issuer must also ensure that no token that has been previously issued is offered again publicly, since this will enable the trustworthiness of the system to be strengthened; in addition, the Physical Validator is able to assume this guarantee function only if it extends to the tokenisation of rights in property. Where, apart from the rights in property, other such rights are to be tokenised and issued, the duplicate issue of tokens by the Token Issuer must be prevented in any event.

Art. 14 sub-para. d obligates Token Issuers to ensure that, where subsequent issue of related rights takes place, a note pertaining to the previous issue is entered. If, for example, the right of use in a bicycle is tokenised during the first issue, when tokenising the title to the bicycle later on, a note must be entered pertaining to the right of use in the bicycle previously tokenised.

This obligation, too, – to the extent that the tokenisation of rights in property is concerned – must be viewed in turn in connection with the obligation of the Physical Validator pursuant to Art. 20 sub-para. a, who must ensure that the customer commissioning the generation of a token may lawfully dispose of the right to be tokenised at the time of generation so as to specifically prevent a conflict of rights that occurs when rights in the same property item are tokenised. The tokenisation of title to and the tokenisation of the right of use in the same property item does not, per se, constitute a conflict of rights in terms of Art. 20 sub-para. a, as long as the lawful person possessing the right of disposal over the tokenised title and the tokenised right of use is the same person. Entering a note pointing to the previous issue having taken place is imperative at the latest upon the issue of tokens covering such related rights.

Art. 14 sub-para. e obligates the Token Issuer to ensure that there are processes in place that are suitable for restoring the allocation of users and issued tokens within a reasonable period of time in the event of a disruption of any kind, including, but not limited to, technical glitches, attacks by third parties, etc.

Re: Art. 15

Art. 15 sets out the special requirements that are applicable to the TT Depositary. By definition, the TT Depository holds the Private Keys of users in safekeeping. As already set out in the comments on the Definitions and Terms, the Private Key enables the person who possesses the power of disposal to decrypt data that has been encrypted using the Public Key, as well as to generate digital signatures and thus carry out transactions.

Consequently, the Private Key enables disposition over the tokens. As illustrated by the example of Bitcoin, tokens exhibit substantial market values, which is why an appropriate degree of care must be exercised in holding one's own Private Keys in safekeeping. This applies all the more when the safekeeping of Private Keys is performed on behalf of third parties in exchange for payment. It should be borne in mind that, owing to the current state of the art, the restoration of Private Keys is not possible in the event they are actually lost. This means that tokenised rights in assets are lost to heirs if the decedent did not make any back-up copies of his/her Private Keys or the decedent's Private Keys cannot otherwise be made accessible upon his/her death.

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

Art. 15 sub-para. a obligates TT Depositaries to take appropriate precautions to ensure that Private Keys are protected, especially against duplication, loss, theft, destruction, etc.

Art. 15 sub-para. b obligates TT Depositaries to hold the Private Keys of customers in safe-custody separately of the TT Depositaries' own. The purpose of this is to ensure that verification is enabled at all times to determine which Private Keys are held in safe-custody on behalf of customers and which Private Keys are part of the TT Depositary's business assets. Consequently, in analogous application of Art. 24 Bankruptcy Rules (KO), the Private Keys of customers held in safe-custody are to be segregated from the bankruptcy estate in the event of bankruptcy on the part of the TT Depositary.

Art. 15 sub-para. c obligates the TT Depositary to ensure that there are processes in place that are suitable for restoring the allocation of customers and Private Keys held in safe-custody within a reasonable period of time in the event of a disruption of any kind, including, but not limited to, technical glitches, attacks by third parties, etc.

Re: Art. 16

The TT Price Service Provider does not have any active role in dispositions, i.e. in exchange and trade transactions, consequently no transaction risk exists. This service provider only collects information (e.g. bid, offer and closing prices for identical tokens) and uses it to derive aggregated information that provides an indication of the price of a token to traders, asset managers and users. The most significant risk in this connection is posed by conflicts of interest and incorrect calculations. This risk is to be countered by TT Price Service Providers being compelled to guarantee that the prices published by them are verifiable and to avoid conflicts of interest in determining pricing. In order to ensure transparency, TT Price Service Providers are also obligated to disclose information to concerned users about transactions with related parties. “Concerned users” refers to all persons who are able to examine the respective price information.

Re: Art. 17

This provision sets out specific obligations pertaining to conduct and the requirements to be satisfied in operating a TT Exchange Office. The operator (in their capacity of TT Service Provider subject to registration) is obligated to set up internal control mechanisms (systems) that ensure that the information described in Art. 17 is always retrievable by third parties.

In this respect, this provision serves to protect users and ensure transparency.

How the TT Exchange Office Operator goes about complying with their obligations is left to them. In any event, the TT Exchange Office Operator must have suitable internal control systems in place.

Re: Art. 18

Art. 18 sets out the special requirements that are applicable to TT Protectors. TT Protectors provide typical fiduciary services relating to a TT System to protect the privacy of users. TT Protectors act in their own name or on behalf of one or more third parties. That is why the government considers it appropriate that these services be provided as set out in the Banking Act (BankG) or the Trustee Act (TrHG) for which other *lex specialis* requirements apply apart from the due diligence obligations that serve to protect users and customers of the Liechtenstein financial centre.

Re: Art. 19

Art. 19 sets out the special requirements that are applicable to Token Generators. Token Generators create rules (software) determining how tokens behave, which interactions are possible, and, in particular, the conditions under which tokens may be transferred.

With this in mind, the Token Generator is to maintain the functionality of the rules (software) up to three years upon transfer to the customer in analogy to warranty rights under the General Civil Code (ABGB). The Token Generator does not have a warranty obligation in respect of the TT System used, but rather may incur liability based on *culpa in eligendo*. This idea is based on the circumstance that TT Systems are not under the control of individuals, and therefore also not that of Token Generators.

Re: Art. 20

Art. 20 sets out the special requirements that are applicable to Physical Validators. Physical Validators perform a central function in the area covered by this Law in which rights to physical property items may be tokenised. The main task is to ensure the link between the property item and the token embodying rights in that property item. Hence, the case is envisaged, for example, in which a user approaches a Token Generator with an order to tokenise rights in a watch, which the user owns.

Art. 20 sub-para. a: The Physical Validator must therefore ensure that the customer commissioning the generation of the token may also lawfully dispose of the tokenised rights in the watch. If, for example, title is tokenised, the Physical Validator must ensure that the customer commissioning tokenisation is also the owner.

The Physical Validator must also ensure that the customer commissioning the generation of a token may lawfully dispose of the right to be tokenised at the time of generation so as to prevent a conflict of rights especially when tokenising rights in the same property item. This also includes verifying whether a partial or full right in a specific property item has been tokenised, thus barring the tokenisation of another partial right or even the entire right due to the absence of lawful disposition over the right.

If, for example, the rightful owner of a watch has previously tokenised the full right "title" to the watch, the Physical Validator must prevent this right from being tokenised once more.

If, say, the right of use in this watch has been previously tokenised by the owner and now the owner wishes to have title to the watch tokenised, the Physical Validator must also verify whether the token that is securitised as a right of use in the watch still falls under the owner's right of disposal as provided for in Art. 7. If this is the case, tokenisation may take place, since the customer commissioning the generation of the token is also the holder of title to the watch and thus may lawfully dispose of the full right to be tokenised. If, however, the token embodying the right of use has already been transferred, the customer seeking to have a token generated for title to the watch no longer has the lawful right of disposal over the full right to be tokenised since a partial right – in this case the right of use – no longer falls under the customer's right of disposal by virtue over the token embodying this right having been transferred.

Consequently, in the view of the government the obligation according to Art. 20 sub-para. b constitutes a key function in TT Systems since the safeguard function intrinsic to it strengthens its trustworthiness in that deliberate or inadvertent conflicts of rights are prevented.

Art. 20 sub-para. c compels the Physical Validator to assume liability for compensation for the event that the person possessing the right of disposal over the token in terms of Art. 7 is unable to successfully assert their claims to obtain the securitised property item on account of the conduct of the Physical Validator.

This provision primarily addresses the following concern: If the owner of the watch in the example above decides to have a token generated to embody title to the watch, according to Art. 20 sub-para. a, the Physical Validator must first verify that he/she actually lawfully disposes of the full right of ownership ("title") at that time before generating the token.

If this is the case, the Physical Validator will issue a confirmation so that generation of the token can take place.

If this token in which title to the watch is securitised were to now be transferred, according to the rules of transfer set out in Art. 7 and Art. 8, title to the watch would also be transferred.

However, the recipient (transferee) of the token in which title to the watch is securitised warrants protection insomuch as it must be ensured that he/she is also able to effectively dispose of the right embodied in the token (title to the watch) in his/her capacity of person possessing the right of disposal over the token as provided for by Art. 7. For example, it must be ensured that the recipient (transferee) of the token embodying title to the watch is also able to actually gain access to the watch itself.

The Physical Validator must ensure this. In the view of the government, the enforceability of this right can be ensured by the Physical Validator taking the property item in which a right is to be tokenised into safe-custody. If, however, the Physical Validator does not take the property item in which a right is to be tokenised into safe-custody, they do not act unlawfully per se. Nevertheless, they must ensure that the person possessing the right of disposal over the token – who is also the person possessing the right of disposal over the right embodied in the token pursuant to Art. 7 – is able to successfully enforce any claims for compensation. In practice, the Physical Validator must either obtain insurance cover or have a guarantee issued, or they must collect suitable security from the customer who has tokenisation performed.

As shown by the example of the tokenisation of title to the watch, a Physical Validator who does not take the watch into safe-custody must obtain insurance cover or other security – presumably at the expense of the customer having tokenisation done – for the event that the customer loses the watch, or pledges or sells it and the recipient (transferee) of the token embodying title to the watch is no longer able to gain access to the watch. In this case, the transferee of the token can still obtain satisfaction from the insured value of the property item. The same applies if the Physical Validator possesses a bank guarantee covering the value of the watch or another equivalent form of security (here, too, presumably at the expense of the customer having tokenisation performed).

If the Physical Validator does not take the property item into safe-custody and also does not take any precautions, and if the efforts of the person possessing the right of disposal over the token to enforce their right are to no avail because the transferor no longer has the property item, the Physical Validator acts unlawfully.

Re: Art. 21

Art. 21 sets out the special requirements that are applicable to a TT Verifying Authority. According to the definitions, a TT Verifying Authority must verify legal capacity and the conditions for disposition over a token.

According to Art. 7, the person possessing the right of disposal over the token also possesses the right of disposal over the right embodied by the token. As to the provisions pertaining to transfer (Art. 7 in conjunction with Art. 8), challenges may therefore arise with regard to the legal capacity and/or other special requirements pertaining to the transferor and transferee.

The example of a vineyard estate that issues a “vintage token” for a future wine crop shows the challenge posed by this. If the “vintage token” is designed so that the transferee actually receives wine, it must be possible to take into account special requirements such as the purchaser’s age. Thus, by using a TT Verifying Authority, a 12-year-old could be prevented from getting their hands on these tokens.

Another example is a person with a firearms permit having their title to a gun tokenised. The verification service performed by the TT Verifying Authority would consist of confirming that the recipient (transferee) of a weapons token actually has a firearms permit.

Verification by the TT Verifying Authority can be done by employing technical means.

Re: Art. 22

In a blockchain system, a TT Identity Service Provider assumes a role similar to that of a trust services provider pursuant to the EEA Signature and Trust Services Act (EWR-SIGVG), the difference being the provider's technology platform. The TT Identity Service Provider must verify the identity and, if necessary, the specific attributes of the natural person or legal entity. Para. 1 stipulates that establishing identity must be done by way of an official photo identification card or other equivalent documentary evidence, or evidence that can be verified where the person or the representative of a legal entity is physically present. The following is conceivable, for example: Reliably documented identification that has taken place previously on the basis of photo identification presented for opening a bank account, or electronic proof of identity issued by another country satisfying equivalent quality criteria. The representatives of legal entities must also furnish proof (e.g. articles of association, corporate charter or a commercial register extract) of their power of representation.

Para. 2 stipulates that establishing one's identity can also be done without being physically present or by way of another method of identification that provides for equivalent certainty in terms of the reliability offered by one's physical presence. This possibility is designed to take account of innovative possibilities that are afforded, particularly by virtue of dynamic technological advances.

Para. 3 describes the requirements to be satisfied by internal procedures relating to the correct allocation of Public Keys to their owner and the safekeeping of customer data. Owing to its high sensitivity, personally identifiable information must be stored securely so as to prevent abuse.

Re: Art. 23

Similar to the provisions of Art. 16 Banking Act (BankG), Art. 23 contains a supervisory stipulation relating to the protection of specific designations used in business names. This is designed to protect users and promote transparency in the financial market.

According to this provision, certain designations, i.e. “TT Service Provider” or “Token Issuer”, for example, may not be used in Liechtenstein unless the TT Service Provider is registered. This does extend to cases in which a name is used that contains a partial designation such as “token”. Art. 23 also does not extend to cases in which a translation of these designations into another language is used in a name.

By virtue of Art. 23, only those TT Service Providers are privileged according to Art. 36 (1) who are entitled to operate TT Services at the time of use of the designation and who have been entered in the TT Service Provider Register pursuant to Art. 41.

The purpose of Art. 23 is also to prevent persons that are not subject to the requirements of the TT-Act from giving rise to any false assumptions pertaining to their entitlement to engage in relevant TT Services. Therefore, Art. 23 serves to secure the conduct of commercial trade and seeks to forestall unfair competition. A company that is not subject to the TT-Act may not gain a competitive advantage over registered TT Service Providers by using a relevant designation and creating the false impression of being subject to this Law.

Here it is immaterial whether protected designations are used on the Internet, in media releases, etc. (deceptive “business advertising”).

Re: Art. 24

In order to protect customers, clarifying the segregation of tokens held by the TT Service Provider in a fiduciary capacity from the TT Service Provider’s own assets is crucial. This is of particular relevance in the event that the TT Service Provider were to go bankrupt since, without a statutory provision, the tokens of customers could, in principle, be claimed by creditors.

Holding in a fiduciary capacity means that the TT Service Provider holds the tokens in its own name in external dealings while securing unambiguous allocation to customers. This can also be done in a separate system.

In the securities sector, there is a similar issue which has been legally resolved in the Banking Act (BankG) by segregating the securities from the depositary’s assets.

A similar wording is used here for TT Systems in order to create clarity and strengthen the protection of customers. Tokens held in safekeeping in a fiduciary capacity are accorded a special status under the law and do not fall under the bankruptcy estate of the TT Service Provider.

What is key here is the distinction drawn as opposed to the deposit business pursuant to the Banking Act (BankG). The deposit business is defined as the acceptance by a bank of funds shown on its balance sheet, with the objective of lending the funds at the bank’s own risk (e.g. loans) or otherwise investing them. The safekeeping of tokens in a purely fiduciary capacity does not constitute deposit business since the tokens are not passed on by the TT Service Provider in the course of making loans, etc. Consequently, the safekeeping of tokens in a fiduciary capacity is more comparable to banknotes that are held in safekeeping in a vault.

According to the current draft of the Law, the holding of tokens on behalf of customers in a fiduciary capacity can only be done by TT Protectors. Nevertheless, the wording of this article has been left open in order to clarify the general application of these protection clauses.

In drafting this article, concrete provisions specifying how tokens are to be held were deliberately omitted, in particular wording specifying “separate safekeeping at all times” in which tokens are segregated from the TT Service Provider’s own assets, as this is virtually not feasible in practice, particularly if a service provider offers transaction accounts for tokens. The key issue for the protection of users is the ability at all times to unambiguously allocate tokens to their lawful owners and therefore the possibility to segregate them from the bankruptcy estate in the event of bankruptcy on the part of the service provider.

Re: Art. 25

The provisions of Art. 24 relating to the holding of tokens in a fiduciary capacity apply accordingly to the safekeeping of Private Keys in the name of the customer so as to have legal certainty vis-à-vis creditors in this case as well in the event of bankruptcy on the part of the TT Service Provider.

Re: Art. 26

TT Service Providers must retain relevant business documents and records (e.g. documents pertaining to customers, business strategies, meetings of executive bodies, etc.) for a period of at least ten years. This is without prejudice to more specific retention periods.

Re: Art. 27

Art. 27 establishes the requirements applicable to outsourcing operational activities. In the group of outsourced tasks, the Law distinguishes between “standard” and “key operational tasks”. According to the *ratio legis*, outsourcing general (non-essential) operational tasks (e.g. operation of a website or a whistle blowing hotline) using vicarious agents is permissible as a general principle as provided for by general civil, criminal, and data privacy and protection law.

Here (2) establishes which tasks are deemed to be important. The result of this is that certain operational tasks cannot be outsourced (e.g. the central agenda of executive management and ultimate decision-making authority, civil and criminal liability, etc.).

Para. 3 stipulates for general and important operational tasks that a TT Service Provider must take adequate precautions to ensure that the requirements of this Law are satisfied. This includes data privacy and protection, information management, etc. The precautions which a TT Service Provider must take in an individual case are in keeping with the principle of proportionality. The following must be taken into account: the specific business model and the resulting risk posed (e.g. to users), and a TT Service Provider’s size and capacity.

Where other laws contain specific stipulations that apply to outsourcing, they are applicable in the capacity of *leges speciales* ((4); cf. for example, Art. 19 Data Protection Act (DSG)).

Re: Art. 28

Like the stipulations of the Securities Prospectus Act (WPPG) pertaining to securities prospectuses, the issue of tokens and their public offering require that sufficient basic information be provided for the interested members of the public.

A quantum of “basic information” is designed to inform interested members of the public about the purpose of the token issue so that informed judgement can be made concerning the associated risks and rewards (cf. Art. 30 (1)). The obligation to provide information pertains to a (commissioned) Token Issuer, not to Token Generators or other persons.

A sufficient quantity of “basic information” is to be provided. The Law makes only general stipulations with regard to the degree of detail to be satisfied by the requisite information (cf., for example, Art. 30 (2)). The appropriate level of information is achieved when an interested purchaser or other persons are able to obtain the requisite details pertaining to the issue, the purpose of same, and the associated risks and rewards in a reasonable amount of time.

It is the responsibility of the issuer to ensure that the information function of Art. 30 can be satisfied in any event.

Basic information is to be made available to the public in good time, i.e. prior to the issue of tokens. The Law does not contain any detailed stipulations pertaining to the place of publication, but rather leaves the decision to the issuer how they inform the interested members of the public. The following may be considered: publication in a newspaper, on the issuer’s website, etc. (cf., for example, Art. 17 (3) Securities Prospectus Act (WPPG)).

The basic information is to be notified to the FMA as well. The FMA is not obligated to perform a formal review to determine whether the basic information complies with the law, so as not to delay the issue of tokens by virtue of the notification obligation. In order to safeguard the reputation of the Liechtenstein financial centre and to protect users, it is important to the government that the FMA be informed of activities and be able to intervene in the event of violations.

Re: Art. 29

Para. 1: This provision is functionally equivalent to Art. 7 Securities Prospectus Act (WPPG) and sets out the formal requirements applicable to basic information pertaining to tokens. In order for basic information to fulfil its designated function, it must be easy to understand and logical (this implies using clear and concise sentences, avoiding complex syntax, using the active voice instead of the passive voice, etc.; if possible, jargon should be avoided).

Para. 2: Basic information may be contained in multiple documents as long as it is clear how the documents are related to one another.

Para. 3: If the Token Issuer uses multiple information documents, they must also make a concise, easy-to-understand summary available that satisfies the minimum requirements according to (3). This "executive summary" is designed to inform the reader of the core content of the individual documents.

Para. 4: This paragraph establishes that the basic information must be drafted and made available in German or English.

Re: Art. 30

This provision is modelled on Art. 8 Securities Prospectus Act (WPPG).

Para. 1 sets out the general minimum details which the basic information must contain, e.g. description of the rights associated with the tokens being issued and the requisite risk warnings (e.g. that investments are not covered by the Deposit Guarantee and the Investor Compensation Act (EAG)).

Pursuant to (2), the Token Issuer is to make a potted summary of their project ("key information") available. Whereas the purpose of the summary set out in Art. 29 (3) is to provide to the reader general information on the issuer's various information documents (this summary need not be provided unless the basic information is comprised of multiple documents, e.g. one document describing the issue and another describing the associated rights), the key information should generally contain a brief final summary of the project and the associated risks. However, key information is to be provided in any event.

It is conceivable that summaries according to Art. 29 (3) and Art. 30 (3) are combined.

(3) and (4) obligate issuers to provide a “legal notice” indicating who is legally and technically responsible for implementing the project.

Basic information should always be kept up to date. The basic information must feature the date of issue ((5)) so that readers can establish when information pertaining to a token project was initially compiled.

Re: Art. 31

The obligation to publish basic information is purposely framed to cover a 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. Also, the willingness of the consumer to read basic information in this case is presumably next to non-existent.

By imposing an obligation to publish basic information and making stipulations pertaining to the content of that information, the government is seeking to establish that correctly informing purchasers is key 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 first exemption clause (para. 1 sub-para. a) provides an opt-out clause for all these applications, subject to the condition that all purchasers waive taking cognisance of the basic information. The second exemption clause is modelled on the exemption clauses of the Securities Prospectus Act (WPPG) involving 150 users. The third exemption clause specifies a volume threshold of CHF 1 million under which the government gives small projects and applications the option of whether they wish to publish basic information.

The Securities Prospectus Act (WPPG) also sets out exemptions for qualified investors. The government is dispensing with a similar wording because, given the broad array of applications, it is impossible to provide a definition of "qualified" that ensures legal certainty.

Sub-para. d is a conflict-of-laws provision, especially regarding the Securities Prospectus Act (WPPG). It goes without saying that the provisions of the Securities Prospectus Act (WPPG) take precedence over those of the TT-Act, and that, as a consequence, basic information pursuant to the TT-Act need not be additionally published. The wording of sub-para. d is deliberately of a general nature since it is conceivable that further obligations in this context will arise at a later point in time.

Para. 2 is modelled on the resale provisions of the Securities Prospectus Act (WPPG).

Re: Art. 32

This article sets out the civil liability incurred by the Token Issuer relating to the disclosure or failure to disclose information and is modelled on Art. 38 Securities Prospectus Act (WPPG). As in the Securities Prospectus Act (WPPG), no upper limit of liability is specified. The amount of compensation is to be determined by the court seized of the matter in an individual case.

Re: Art. 33

This provision is based on Art. 39 Securities Prospectus Act (WPPG); it sets out joint and several liability for cases in which multiple persons are responsible for damage or loss caused by incorrect, misleading or incomplete information.

Re: Art. 34

The place of jurisdiction provision contained in Art. 34 is functionally equivalent to Art. 40 Securities Prospectus Act (WPPG).

Re: Art. 35

Cf. the functionally comparable statute of limitations pursuant to Art. 41 Securities Prospectus Act (WPPG); Art. 35 TT-Act is modelled on this provision and the other existing supervisory statutes. This provision is designed specifically to provide for enhanced legal certainty and the protection of investors. Art. 35 is in reference to the failure to create basic information and the creation of false or erroneous basic information.

Re: Art. 36

(1): The TT Service Providers indicated in (1) are obligated to register with the FMA prior to providing their services. Consequently, making application for registration is to be done before commencing the provision of the relevant TT Services. Registration is necessary if TT Services are to be provided on a commercial (professional) basis in Liechtenstein. Similar provisions of the Business Act (GewG) or the Banking Act (BankG) can be consulted for the interpretation of the term “on a commercial basis” / “on a professional basis”. (1) subjects only certain service providers to the registration requirement; the itemisation in (1) is exhaustive. This is intended to ensure transparency in the Liechtenstein financial centre; in the process, TT Service Providers are afforded access to a “seal of quality”. Only those providers who satisfy the applicable general and special statutory requirements – which differ according to category of service – are entitled to entry in the TT Service Provider Register.

(2): TT Service Providers who are not listed in (1) (e.g. Token Generators or Price Service Providers) may voluntarily register with the FMA – in terms of obtaining a seal of quality. However, they are under no obligation to do so. If the service providers listed in (2) register, they must categorically comply with the same requirements as the TT Service Providers listed in (1) (Art. 13 (5)).

(3): This paragraph specifies what formal minimum details must be included in an application according to (1) (e.g. address of the TT Service Provider).

(4): This paragraph itemises which supporting documents must be included with an application for registration. Here, the Law draws a distinction between natural persons and legal entities, and specifies the requirements applicable to each.

In (4) sub-para. a point 2, the Law requires that the applicant submit suitable certifications showing that no grounds for refusal are present pursuant to Art. 13 (1) at the time application is made. As a result, the applicant is given the option of submitting other suitable evidence or supporting documents, e.g. references, evidence of professional experience and credentials, police clearance or certificate of good conduct, and the like.

Para. 5: Application for registration can be made with the FMA in writing by postal letter or electronically. The supporting documents stipulated in (4) preclude making application orally or over the telephone.

In addition, (5 also specifies that supporting documents need not be submitted in the original, and that certified copies also suffice for making application. If, however, the FMA has any doubts concerning the authenticity of the documents submitted, it may request that the applicant submit the originals. In this case, a supporting document will not be deemed to have been submitted until the original has been received by the FMA.

Para. 6: This provision sets out an (unconditional) obligation on the part of TT Service Providers to provide information. They are obligated to report all changes relevant to regulatory requirements to the FMA immediately upon the occurrence of same where they pertain to the facts set out in paras. 2–5.

Para. 7: This provision establishes that financial intermediaries who have already been approved by the FMA must register with the FMA if they wish to engage in an activity on a TT System. However, these financial intermediaries need not resubmit evidence of their qualifications which they submitted previously for obtaining their FMA approval. In other words, a simplified registration procedure exists for financial intermediaries. However, the government believes it is important to emphasise that financial intermediaries, too, must adopt their internal procedures in line with TT Systems.

Re: Art. 37

Para. 1: The FMA must review all the application documents to determine whether an applicant complies with all statutory requirements for providing TT Services. The Law allows the FMA a review period of (up to) three weeks.

If all the requirements are satisfied in an individual case, the applicant is to be entered in the TT Service Provider Register; the applicant has a subjective legal entitlement to entry in the register in this case. Entry in the register, not notification pursuant to Art. 36 (3., is constitutive for establishing the right to provide TT Services in Liechtenstein pursuant to Art. 36 (1.

The FMA must notify the applicant upon their successful entry in the register; said act of notification is of a declarative nature.

The FMA may make entry in the register subject to certain conditions and obligations in the interests of protecting users and the transparency of Liechtenstein's financial centre. For example, the FMA may stipulate that certain information is to be provided from time to time, or impose restrictions on specific services to be provided, and so forth.

Para. 2: No administrative decision needs to be issued for entry in the register, i.e. no ruling or similar is handed down. If, however, the FMA refuses application for entry in the register (the applicant has not satisfied all requirements), it must prohibit the applicant from engaging in services. In this case, no entry in the register may be made.

Despite any negative outcome of an applicant's attempted registration, they are not prevented from resubmitting their (improved or modified) business model to the FMA for review.

Re: Art. 38

Art. 38 establishes the conditions under which registration expires. Expiration of a registration must be viewed as an abolishment of the permission to provide TT Services according to Art. 36. (1. It occurs by virtue of law, without any further administrative steps being required.

Re: Art. 39

Registration is revoked if a TT Service Provider systematically, i.e. persistently and grossly, violates their legal obligations or does not comply with requests of the FMA to restore the proper ("lawful") condition. In this case, even a serious breach of duty may justify revocation. Revocation of a licence goes into effect ex nunc, i.e. upon entry into legal force of the FMA's decision.

The FMA must set out grounds for revoking registration and must publish its decision upon the entry thereof into legal force, and notify it by way of the TT Service Provider Register as set out in Art. 41.

Re: Art. 40

Para. 1 establishes that cancellation of registration must result in the company immediately discontinuing its operations as a TT Service Provider. Since TT Service Providers like TT Depositaries and TT Protectors provide asset management-related services for customers, upon discontinuing operations they must ensure that the interests of customers are not impaired as a result of discontinuation. Informing the FMA about these precautions and the FMA's possibilities for intervening are designed to benefit customer protection.

Re: Art. 41

Here the FMA is obligated to establish a publicly accessible register and to maintain it. The register must be accessible by everyone free of charge or be accessible online ((2). The registered TT Services offered by every TT Service Provider must be entered in the register ((1).

In (2 reference is made to Art. 7 Data Protection Act (DSG) in particular, according to which the data processed in the register must be correct and current at all times. If the FMA gains knowledge of a situation requiring that an entry be amended, it must correct the entry without undue delay.

Re: Art. 42

Art. 42 establishes which authorities are competent for enforcing this Law. The concrete division of responsibilities and the powers result from specific ordinances.

Re: Art. 43

This provision underscores official secrecy according to which the competent authorities, their staff, experts and other persons consulted by such bodies are subject to a comprehensive obligation to maintain confidentiality. This obligation to maintain secrecy remains in full force and effect if a person no longer works for an authority or body.

Any disclosure of information that is subject to official secrecy is permissible only in the cases provided for by law (para. 2). Special provisions are set out in para. 3 and 4. These stipulations are in accordance with applicable provisions in other substantive laws.

Re: Art. 44

In order to secure the effectiveness of regulatory supervision, Art. 44 obligates the relevant authorities and bodies to render mutual administrative assistance, especially where this is expedient to perform their duties under this Law.

Re: Art. 45

With regard to Art. 6 DSGVO, this article creates the requisite statutory basis to authorise the competent national authorities and bodies to process personally identifiable information and to engage in the task-related exchange of information.

Re: Art. 46

This article sets out in detail the tasks of the FMA. It is responsible for carrying out and cancelling registrations, maintaining the TT Service Provider Register and prosecuting violations. The FMA has certain powers to this end that it can exercise either directly (i.e. by independently taking action) or in concert with other competent authorities and bodies.

Para. 2 establishes a general clause for the powers required for the FMA’s tasks. It contains a catalogue of illustrative examples of the FMA’s regulatory powers, however, the list is not exhaustive. This list also corresponds to the provisions contained in parallel substantive laws.

Para. 3 contains the rules for the assumption of costs that already follow from the Financial Market Supervision Act (FMAG); this is repeated for the sake of completeness and clarity under the supervisory provisions to this Law. Among other things, it establishes that service providers who provide TT Services without being registered and thus trigger action on the part of the FMA pursuant to para. 6 must assume the costs of the proceedings.

Para. 4 contains the usual imperative directed to the FMA to take the necessary action to restore the lawful state of affairs and to remedy abuses.

In the event a TT Service Provider is in financial distress or is responsible for other serious irregularities that do not yet entitle the FMA to revoke the service provider’s registration, the FMA is authorised to place it under government supervision for a limited period of time (para. 5). Supervision is to be done by an “expert supervisor” under the control and directives of the FMA. The expert supervisor is appointed by the FMA in the event that a danger is posed to the interests of users or creditors. The task of the supervisor in particular is to oversee the executive bodies of the TT Service Provider; in so doing, the supervisor is able to prohibit the implementation of risky decisions taken by them. This provision is also in line with current legal practice embodied in other substantive laws.

According to Art. 36. para. 1, the provision of TT Services is subject to prior registration. In order to bring this prohibition standard into effect, unauthorised operation was not only made a punishable offence, the FMA was also authorised to investigate relevant suspicious cases (for example, as the result of a complaint) (para. 6). If necessary, the FMA can order that the provider immediately cease unauthorised operation and refrain from other actions that are associated with unauthorised operation (e.g. cease-and-desist orders for advertising, shutting down a website, and the like).

Re: Art. 47

The standard serves the purpose of clarification. TT Service Providers must pay the fees and charges for registration by the FMA, as set forth in the annexes to the Financial Market Supervision Act (FMAG).

Re: Art. 48

Art. 48 provides access to a comprehensive review procedure for persons who are affected by a decision or ruling of the FMA, in line with Art. 43 para. 1 Constitution of the Principality of Liechtenstein (LV) and Art. 6 para. 1 European Convention on Human Rights (ECHR). In so doing, the article sets out the usual requirements applicable to legal remedies in regulatory proceedings. General civil and criminal procedure provisions apply to legal remedies in civil and criminal proceedings.

Paragraph 4 corresponds to parallel stipulations in other substantive laws; it stipulates that the National Administration Act (LVG) applies to the conduct of public-law proceedings falling under the scope of this Law.

Re: Art. 49

Art. 49 paras. 1 and 2 cite various sanctionable violations that are subject to payment of a fine of up to CHF 20,000 or CHF 30,000, depending on the severity of the violation. This itemisation of definitional elements covers all the violations of this Law. They are intended to be effective and appropriate and act as a deterrent. The amount of the fines is modelled on FinTech regulations in European countries (in particular Austria’s Alternative Financing Act (AltFG)).

Paras. 3 to 5 establish the criminal liability applicable to legal entities. The persons responsible for the legal entities are to be prosecuted where they have acted personally (para. 3) or have facilitated the commission of a violation by an employee due to a failure to act within their organisation (para. 4). This stands to reason so that penalties are not imposed exclusively on the natural persons acting on behalf of a legal entity; any action can also be taken as needed exclusively against the legal entities themselves applying the principle of proportionality (para. 5). Hence, these stipulations are in line with established provisions in other substantive laws.

According to para. 6, only half of the applicable penalty may be imposed where a violation is the result of negligent conduct. The Law covers cases of both slight and gross negligence.

Re: Art. 50

Where a violation is attributable to a legal entity and not to a natural person, the natural person who acted or was obligated to act in the name of the legal entity is to be prosecuted and punished as the perpetrator (“accountable person”).

Re: Art. 51

Para. 1 establishes the application of the provisions pertaining to the issuing of tokens and the obligation to publish basic information upon the entry into force of this Law. This wording is intended to establish that tokens which were initially offered publicly prior to the entry into force of this Law are not subject to the obligations imposed by this Law, also where the issuing of tokens continues subsequent to the entry into force of this Law.

Para. 2 enables tokens that were generated prior to the entry into force of this Law to be placed under the legal certainty provided by the provisions pertaining to the disposition of tokens in Chapter II.

Para. 3 designates an appropriate period of six months within which TT Service Providers who already engage in the provision of services must register with the FMA.

Amendment of the Due Diligence Act (SPG)

Re: Art. 3

The scope of application of the Due Diligence Act (SPG) is expanded by the due diligence-relevant TT Service Providers. TT Exchange Office Operators are to be viewed as a supplement to the exchange bureaux pursuant to Art. 2 para. 1 subpara. l Due Diligence Act (SPG) so as to cover the broad scope of the TT-Act.

Re: Art. 23

This article establishes the competence of the FMA for supervision and enforcement relating to TT Service Providers in respect of their due diligence obligations.

Amendment of the Financial Market Supervision Act (FMAG)

Re: Art. 5

By referencing the TT-Act, this article establishes the competence of the FMA.

Re: Annex 1

TT Service Providers must pay a fee for making application for registration, as well as for any cancellation and expiration of their registration. The amount of the fee payable is in line with comparable services, e.g. fiduciary agent, patent attorney or auditor licences.

Re: Annex 2

An annual fee of CHF 500 is established for TT Service Providers in analogy to other activities supervised by the FMA (e.g. auditors).

Amendment of Section 81a Persons and Companies Act (PGR) (Final Part)

This proposal for a new section 81a Final Part, Persons and Companies Act (PGR) introduces the legal device of the uncertificated rights to Liechtenstein Law and creates the interface between securities law and the TT-Act. This creates the possibility of issuing uncertificated rights in the form of tokens on a decentralised database and transferring them there. TT Systems are perfectly suited for issuing and transferring uncertificated rights 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, Persons and Companies Act (PGR) is modelled on Art. 973c of the Swiss Code of Obligations, however, it extends further in various aspects.

Para. 1: Uncertificated rights are defined as rights with the same function as certificated securities. Pursuant to section 73 Final Part, Persons and Companies Act (PGR), certificated securities are characterised in that the right securitised by way of a charter certificate "cannot be utilised, asserted, or transferred to others". In other words they are subjective legal rights that can be submitted to independent transfer and proof of authorisation rules by way of chartering. Uncertificated rights are dematerialised securities for which the security certificate is replaced by the "uncertificated rights ledger" and entry in the ledger is subject to independent transfer and proof of authorisation rules.

Para. 1 grants the obligor (issuer) the authorisation to issue uncertificated rights. The obligor may convert existing certificated securities into uncertificated rights if this is provided for in the conditions of issue or the articles of association, or the beneficiaries have given their consent. This is subject to the condition that the certificates in circulation are returned or cancelled; if the obligor fails to do this, double compensation may be sought.

Para. 2: The obligor is compelled to maintain a record, the so-called "uncertificated rights ledger", of the uncertificated rights issued by him or her. This Law does not impose any special requirements with regard to how this ledger is to be maintained; it is sufficient for a recorded entry to show the number or denomination of the uncertificated rights issued and the creditors. As a matter of course, the uncertificated rights ledger can also be maintained electronically, in particular also as a decentralised database within the meaning of the TT-Act, where uncertificated rights are issued directly in the form of tokens. The uncertificated rights ledger does not affect the requirements to be satisfied by share registers for registered shares or share ledgers for bearer shares.

Para. 3: Pursuant to para. 3, uncertificated rights are created upon entry in the uncertificated rights ledger and continue to exist only in accordance with said entry. This does not imply that a new right is created upon entry in the uncertificated rights ledger, but rather an existing claims or membership right is subjected to the proof of authorisation and transfer rules applicable to uncertificated rights. Entry in the uncertificated rights ledger is the functional equivalent of transferring a certificate to the first taker when securities are issued. The creditor, who is to be entered in the uncertificated rights ledger according to para. 3, also refers to the first taker, i.e. the issuer or, for example, in the context of a firm takeover, a financial intermediary.

Para. 4: Securities are transferred by way of transferring the certificate (including endorsement or a written declaration of assignment, where necessary). In the case of uncertificated rights, transfer or grant of limited rights in rem takes place by way of entry in the uncertificated rights ledger. If the uncertificated rights ledger is maintained as a decentralised database, transfer or bailment of uncertificated rights (or of the tokens representing them) is done exclusively as provided for by this Law. This also means specifically that assigning uncertificated rights is no longer possible.

Para. 5: Unlike non-securitised claims, a good-faith purchase of securities is possible, the colour of law or appearance of right (*fumus bonis iuris*) being based on possession of the certificate (including a formally uninterrupted endorsement chain, as applicable). In the case of uncertificated rights, entry in the uncertificated rights ledger takes the place of the possession of a certificate. A purchaser who in good faith makes a purchase from a person shown in the uncertificated rights ledger is to be protected when making this purchase even if that person was not authorised to dispose of the rights under substantive law.

Para. 6: The uncertificated rights ledger or the decentralised database is also the point of reference for the proof of authorisation rules applicable to uncertificated rights. The legitimate creditor or the creditor authorised to dispose of the uncertificated rights is whoever is entered in the uncertificated rights ledger as such. The debtor must make payment to this person and is discharged from their obligation by making payment, even if this person does not possess any legal title in substantive law terms.

Amendment of the Business Act (GewG)

Re: Art. 3

Art. 3 is supplemented by sub-para. s. In so doing, it is stipulated that, under the TT-Act (Art. 36 para. 1), registered service providers are only subject to the licensing and supervisory provisions of the TT-Act and not the Business Act (GewG). This is designed to prevent TT Service Providers from being subjected to the unnecessary burden posed by regulatory duplication.

As such, the TT-Act is a *lex specialis* in relation to the Business Act (GewG). The exemption according to Art. 3 sub-para. s Business Act (GewG) applies only if and to the extent that service providers provide TT Services in the capacity of TT Service Providers pursuant to Art. 36 TT-Act. If TT Service Providers also provide other services on a commercial or professional basis (e.g. trade in goods), they are to be assessed in accordance with the Business Act (GewG) or other professional codes.

Following the principle of factual proximity, the exemption of TT Service Providers is modelled on the example of Art. 3 sub-para. I Business Act (GewG), according to which banks, securities firms and insurance companies are also exempted from the Business Act (GewG); these companies are subject to *lex specialis* supervisory regulations of financial market law and supervision by the FMA.

5. CONSTITUTIONALITY / LEGAL ISSUES

This Law does not contravene any constitutional provisions.

6. GOVERNMENT BILLS

6.1 Law Concerning Transaction Systems Based on Trustworthy Technologies (Blockchain Act; TT-Act; VTG)

Law

from ...

on Transaction Systems Based on Trustworthy Technologies (Blockchain Act; TT-Act; VTG)

I give my consent to the following resolution passed by the Parliament:

I. General Clauses

Art. 1

Object and Purpose

The purpose of this Act is to protect users on TT Systems and to ensure their trust in digital rights. It regulates the registration and supervision as well as the rights and obligations of service providers who perform activities on TT Systems.

Art. 2
Scope

1) This Act applies to TT Service Providers.

2) The provisions of this Act concerning the power of token disposal and the disposal over tokens in accordance with Chapter II apply if either:

a) tokens are generated or issued by a TT Service Provider that is subject to this Act, or

b) the Law is explicitly declared applicable.

3) Other statutory regulations, including Persons and Companies Act (PGR), the General Civil Code, financial market legislation, and data protection legislation together with Due Diligence legislation remain reserved.

Art. 3
Trustworthy Technology (TT)

1) Trustworthy technologies within the meaning of this Act are technologies that ensure the integrity of tokens, their unambiguous allocation to the owner whom possesses the power of disposal and their disposal without an operator.

2) At the same time, these technologies function as an operator responsible for quality and integrity.

3) The Government may regulate further details according to this Act through ordinance.

Art. 4

Exemptions from Scope

This Act shall not apply to:

a) the state, municipalities and/or associations of municipalities, if they are acting in their capacity as authorities; or

b) TT Systems, which are only available to a closed user group.

Art. 5

Definitions and Designations

1) For the purposes of this Act:

1. “Token”: Information on a TT System that can embody fungible claims or membership rights to an individual, goods, and/or other absolute or relative rights and ensuring the allocation to one or more Public Keys;
2. “Public Key”: Consists of a sequence of characters representing a unique publicly accessible address contained in a TT System to which tokens can be uniquely allocated;
3. “Private Key”: Consists of a sequence of characters that can be used alone or with other Private Keys enabling the disposal over a Public Key;
4. “Users”: Persons using TT Services;
5. “Token Issuance”: The public offering of tokens;
6. “Basic Information”: Information about tokens to be offered to the public, enabling the user to make an informed judgement about the rights and risks associated with the tokens as well as the service providers involved;
7. “TT Service Provider”: A person who carries out one or more activities in accordance with (8)-(16);

8. “Token Issuer”: A person who carries out the activity of Token Issuance in his own name or commercially on behalf of third parties;

9. “Token Generator”: A person who generates one or more tokens and makes them available via a TT System;

10. “TT Depositary”: A person who provides Private Key depositary services on TT Systems for third parties;

11. “Physical Validator”: A person who ensures the enforcement of rights relating to property, in terms of Property Law, embodied in token on a TT System;

12. “TT Protector”: A person who holds tokens on TT Systems in their own name on account for a third party;

13. “TT Exchange Office Operator”: A person who exchanges legal tender for tokens and vice versa, as well as tokens for tokens;

14. “TT Verifying Authority”: A person who verifies the legal capacity and the requirements for the disposal over a token;

15. “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;

16. “TT Identity Service Provider”: A person who identifies the person in possession of the right of disposal related to a Public Key and records it in a directory;

17. “TT Systems”: Transaction systems that ensure the secure exchange and secure storage of digital representations of rights, as well as the service provisions based on those systems using trustworthy technologies in accordance with Art. 3;

2) The government can define the terms according to (1) in more detail by ordinance.

3) The designations of persons and functions used in this Act, including usage of the pronoun “he,” apply equally to members of the female and male sexes.

II. Disposal over Tokens

Art. 6

Power of Disposal and Right of Disposal

1) The Private Key holder has the power of disposal over the token. It is further assumed that the person possessing the power of token disposal also has the right to dispose of the token.

2) Articles 8, 10, 11 and 12 also apply correspondingly to tokens that do not embody any rights.

Art. 7

Effects of Disposal

1) Disposal over the token by the person possessing the right to dispose of the token results in the disposal over the right embodied by the token.

2) The Token Generator shall take appropriate measures to ensure:

a) that the disposal over a token directly results in the disposal over the embodied right, and

b) that competing disposal over the embodied right are excluded both under the rules of the system and the provisions of applicable law.

3) The transfer of the right of disposal over the token is deemed to be a disposition.

Art. 8
Requirements, Irrevocability and Finality

1) The lawful disposal over tokens requires:

a) the disposal in accordance with the rules of the TT System;

b) the declaration of the transferor and the transferee that they wish to transfer respectively receive the power of disposal over the token; and

c) the transferor’s right of disposal, where the requirements for transfer in “good faith” according with Article 10 are not satisfied.

2) If a token is issued without reason or a subsequent reason fails to exist, the revocation shall be accomplished in accordance with the provisions of the Enrichment Law (§§ 1431 ff. General Civil Code (ABGB)).

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

a) was introduced into the system prior to the commencement of the legal proceedings, or

b) was introduced into the system after the initiation of the legal proceeding and was executed on the day of the proceeding’s openings, provided that the accepting party proves that he was without knowledge of the proceedings openings or would have remained without knowledge upon the exercise of due diligence.

Art. 9

Legitimisation

If the token embodies a right of claim or membership, the person authorised to dispose of the token against the obligor shall be deemed to be the legal owner of this right. By payment, the Obligor is withdrawn from his obligation against the person who has the power of disposal, unless he knew, or should have known with due care, that he is not the lawful owner of the right.

Art. 10

Right of Disposal in Good Faith

Anyone who is granted the right to dispose of tokens for a fee in accordance with the rules of the system is protected in his right to dispose, even if the transferor is not authorised to dispose of the token, unless the transferee knew or should have known, with due care, that the transferor was not authorised in his disposal.

Art. 11

Applicability

The regulations of this Act on the right of disposal and the disposal over tokens shall apply if:

a) the tokens generated or issued by a TT Service Provider fall under Liechtenstein Law in accordance with Art. 2, or

b) this Act is explicitly declared applicable.

Art. 12

Jurisdiction

If Liechtenstein Law is applicable according to Art.11, the token is considered to be an asset located in Liechtenstein.

III. Requirements for TT Service Providers

A. General Requirements

Art. 13

Personal Requirements applicable to TT Service Providers

1) A natural person may only perform TT Services in accordance with Art.36 (1) provided that the following conditions are met:

a) he/she possesses full legal capacity; and

b) he/she is reliable.

2) A legal entity or registered partnership may only perform TT Services in accordance with Art.36 (1) if the members of the management are reliable.

3) Reliability within the meaning of subsection (1) (b) be deemed to be present if:

a) a natural person has not been convicted by a court of law for fraudulent bankruptcy, damage to third party creditors, preferring of a creditor with fraudulent intend, grossly negligent interference with creditor’s interests (§§ 156 to 159 Criminal Code), or has been sentenced up to three months' imprisonment or a fine of more than 180 daily rates for any other Law and the conviction has not been expunged; and

b) there are no other reasons for serious doubt as to the reliability of the natural person.

4) Irrespective its legal form, a TT Service in accordance with Art. 36 (1) may only be provided if a TT Service Provider:

a) has a clear organisational structure with clearly defined, transparent, and coherent areas of responsibility, as well as procedures for dealing with conflicts of interest;

b) has written internal control mechanisms that are appropriate in terms of the type, scope, and complexity of the TT Services provided, including ensuring comprehensive documentation of these mechanisms;

c) can prove a minimum capital of CHF 100,000 or equivalent security; and

d) fulfils the special requirements of Chapter III B, if applicable.

5) For TT Service Providers, according to Art.36 (2), who voluntarily register in the TT Service Provider register, the same general requirements set out in this article apply.

6) The government may further regulate details by ordinance. In particular, it may also enforce other special requirements for individual TT Service Providers in accordance with Chapter III B.

B. Special Requirements for Individual TT Service Providers

Art. 14
Token Issuer

Token Issuers must have internal control mechanisms in place to ensure the following;

a) the disclosure of basic information in accordance with Chapter III D at any time during, and for at least ten years after, the token issuance;

b) the execution of the token issuances in accordance with the order;

c) the prevention of multiple token issuances regarding the same rights;

d) a remark about the issuance that has already taken place in the case of a subsequent issuance of related rights;

e) the maintenance of the provided services in the event of interruptions during the Token Issuance (business continuity management).

Art. 15
TT Depositary

TT Depositaries must have internal control mechanisms in place to ensure the following:

a) the establishment of appropriate security measures protecting customers of the TT Depositary from the loss or misuse of Private Keys by unauthorized third parties;

b) the separate safekeeping of customer's Private Keys from the business assets of the TT Depositaries; and

c) the maintenance of the services in the event of interruptions (business continuity management).

Art. 16

TT- Price Service Provider

TT Price Service Providers must have internal control mechanisms in place to ensure the following:

a) the transparency of the published prices;

b) the prevention of conflicts of interest in relation to pricing; and

c) the disclosure of information to affected users regarding transactions concerning related parties.

Art. 17

TT Exchange Office Operator

TT Exchange Office Operators must have internal control mechanisms in place to ensure the following:

a) the availability of the current market prices of the traded tokens;

b) the disclosure of the purchase and sale prices of the traded tokens.

Art. 18

TT Protector

TT Protectors are required to be licenced according to the Trustee Act or the Banking Act.

Art. 19

Token Generator

Token Generators must have internal control mechanisms in place which ensure the technical functionality of the generated tokens during token generation and for the period of three years subsequent to token generation.

Art. 20

Physical Validator

Physical Validators must have internal control mechanisms in place to ensure the following at all times:

a) that the ordering party of the token generation is the legitimate owner of the property at the time of the token generation;

b) the avoidance of a conflict of rights concerning the same item; and

c) assignment of liability in the event that rights to property guaranteed by the Physical Validator cannot be enforced in accordance with the contract. He must also ensure that the person possessing the power of token disposal has a direct claim against either the Physical Validator's insurance company or the insurance company for the specific property item.

Art. 21

TT Verifying Authority

TT Verifying Authorities must have internal control mechanisms in place to ensure the necessary reliability of the testing services they provide at all times.

Art. 22
TT Identity Service Provider

1) A TT Identity Service Provider, or a person/entity acting as its agent, must establish the identity of the natural persons or representatives of the legal entity whom are physically present, by means of official photo identification documents or other evidence equivalent in reliability, whether documented or to be documented. Representatives of legal persons additionally have to provide an evidence of their power of representation.

2) If the issuance does not take place in person, other methods of identification offering equivalent certainty as to the reliability of personal presence may be used.

3) In addition, TT Identity Service Providers must have internal control mechanisms in place which:

a) ensure the correct allocation of Public Keys to the rightful holder at all times; and

b) guarantee the secure storage of customer data.

C. Organisational Provisions

Art. 23
Designation Protection

1) Designations suggesting an activity in accordance with Art. 36 (1) may only be used in the company name, designation of the business purpose, and/or

in business advertising for those service providers that are entered in the TT Service Provider register in accordance with Art. 41.

2) The government can further regulate details by ordinance.

Art. 24
Safeguarding Requirements

1) Tokens held in a fiduciary capacity do not fall into the bankruptcy assets of the TT Service Provider in the event of bankruptcy. Rather, these tokens are separated out in the customer's favour, with reservations 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. Further, Tokens must remain identifiable in such a way that they can be allocated to the individual user at any time with regard to the individual user’s respective share.

2) 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 Art. 46 (5).

3) In the event of enforcement against his TT Service Provider, the user has the right to appeal (Art. 20 of the Execution Law), if the enforcement relates to the amounts secured in accordance with (1). 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 (Art. 41 of the Bankruptcy Rules (KO)).

Art. 25
Custody of Private Keys

Private 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 shall not be considered part of the bankruptcy estate in bankruptcy proceedings concerning the assets of the TT Service Provider, but rather shall be segregated for the benefit of the client, subject to any claims of the TT Service Provider.

Art. 26
Retention Period

1) A TT Service Provider must keep records and supporting documents relevant for the purposes of this Act for at least ten years.

2) More specific legal obligations remain unaffected.

Art. 27
Outsourcing

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 outsourcing does not lead to a delegation of management tasks; and/or

c) the obligations of the TT Service Provider under this Act remain unchanged, provided that the general and specific requirements in accordance with Art. 13 or Chapter III B under this Act are still fulfilled.

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 to third parties must take adequate precautions to ensure that the requirements of this Act are met.

4) Special legal regulations and arrangements on outsourcing are not affected.

D. Basic Information on Token Issuance

Art. 28

Publication of Basic Information

Subject to the following articles, tokens may only be issued in Liechtenstein if the Token Issuer carrying out the Token Issuance has previously published the basic information on the public offering of tokens and has reported them to the FMA.

Art. 29

Form and Language of the Basic Information

1) Basic information in accordance with Art.28 must be provided in an easy to analyse and comprehensible form.

2) Basic information can be provided in one or more documents.

3) If basic information consists of several documents, the Token Issuer must publish a short and easily comprehensible summary providing information about the Token Issuer and the tokens to be issued.

4) Basic information must be written and made available in German or English.

Art. 30

Contents of Basic Information

1) In particular, the basic information must contain the following:

a) information about the tokens to be issued and the related rights;

b) a description of the technologies used;

c) designation of the TT System used;

d) a description of the purpose and nature of the underlying legal transaction of the Token Issuance;

e) a description of the purchase and transfer conditions of the token;

f) information about the risks associated with the purchase of tokens;

g) a risk warning explaining that investments are not covered by the Deposit Guarantee Act and Investor Compensation Act (EAG).

h) in issuing rights to property:

1. evidence of a registered Physical Validator witnessing ownership of the property, and
2. a confirmation from a registered Physical Validator that the rights issued are also enforceable according to basic information.

2) The basic information furthermore contains a summary, which provides brief and easily comprehensible key information in the same language in which the basic information was originally created. The summary must also include warnings that:

a) it only serves as an overview of the following basic information;

b) the purchaser must read all basic information before making the investment; and

c) those persons who have assumed responsibility for the summary, including a translation thereof, or from whom its issuance originated, can be held liable, but only in the event that the summary is misleading, inaccurate or contradictory when read together with the other parts of the basic information.

3) The basic information must specify names and functions of the actors involved. In the case of legal entities, the company name and registered office of the actors responsible for the content must be recorded. Further, the basic information must include a statement by these persons, companies, or other legal entities that, to their knowledge, the information is correct and no essential details have been omitted.

4) The basic information must include information on the names and functions of companies, and other legal entities involved, including the company

name and registered office of those responsible for the technical and legal functionality of the tokens.

5) The basic information must bear the date of issue and be signed by the Token Issuer.

6) Addendums to Basic Information

a) Any important new circumstance, significant inaccuracy, or imprecision in relation to the details contained in the basic information, which could influence the valuation of the tokens issued, and which are determined after the initial publication of the basic information, must be mentioned in a basic addendum.

b) The addendum must be published and reported to FMA within a maximum of seven working days.

c) In addition, the summary and any translations thereof must be supplemented by the information contained in the addendum.

7) The government can regulate details by ordinance.

Art. 31
Exemptions

1) The obligation of Art.28 does not apply to a public offer of tokens if one of the following exemptions applies:

a) if all buyers have verifiably disclaimed the basic information prior to purchasing the token;

b) if the offer is directed at less than 150 users;

c) if the selling price of the total issuance does not exceed CHF 1 000 000 or the equivalent value in another currency, calculated over a period of 12 months;

d) if there is a pre-existing obligation to publish qualified information about the public token offer under other laws.

2) At each subsequent public resale of tokens, no further basic information shall be published if:

a) the basic information in line with Art. 28 has already been published; and

b) the Issuer, or the person responsible for producing the basic information, has agreed to its use in a written agreement.

Art. 32
Liability

1) If details in the basic information, in accordance with this Act, are incorrect or incomplete, or the preparation of basic information ensuring compliance with these regulations is omitted, the responsible persons, in accordance with Art. 30 (3), must be held liable to each user for the damage caused to the user, unless they can prove that they have applied the care of a reasonably prudent businessman in the preparation of the basic information. Damage is only considered to be direct suffered damages, not speculative damages related to the loss of profits.

2) The persons referred to in (1) must also be liable for their employees, agents, and sub-contractors, unless they can prove that they have applied due care required under the circumstances in the selection, instruction, and monitoring of these employees, agents, and/or sub-contractors.

3) The liability, according to (1) and (2), can neither be disclaimed nor limited in advance in an attempt to disadvantage users or avoid liability for intent and gross negligence.

4) These responsible persons are only liable for details in the summary, including its translations, if these details are misleading, incorrect, or contradictory in connection with other parts of the basic information or these details fail to convey all key information. Further, the summary must contain a clear warning notice regarding this liability.

Art. 33
Solidarity and Recourse

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.

Art. 34
Place of Jurisdiction

The Court of Justice shall have jurisdiction for claims of the transferee of token regarding the legal relationship with the Token Issuer, who publicly offered token within the country.

Art. 35
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, three years from the date of the harmful act.

IV. Registration and Cancellation

A. Compulsory Registration

Art. 36

Compulsory Registration

1) The following TT Service Providers must apply in advance in writing with the FMA for entry in the TT register, if they commercially provide at least one of the following TT Services in Liechtenstein:

a) Token Issuers;

b) TT Protectors;

c) TT Depositaries;

d) TT Exchange Officer Operators;

e) Physical Validators;

f) TT Identity Service Providers.

2) The following TT Service Providers may voluntarily apply with the FMA for entry in the TT register, if they commercially provide at least one of the following TT Services in Liechtenstein:

a) Token Generators;

b) TT Verifying Authorities;

c) TT Price Service Providers.

3) An application with the FMA under (1) and (2) for entry in the TT Service Register under Art. 41 must include:

a) Information about the intended TT Service;

b) Address of the applicant’s registered office or place of residence;

c) Information regarding the legal nature of the applicant, in the event that the applicant is a legal entity or partnership.

4) The application must be accompanied by the following documents:

a) for natural persons:

1. Documentation showing proof of the applicant’s first and last name, place of residence, age and nationality; and
2. Evidence that the applicant is reliable within the meaning of Art. 13 (3).

b) for legal entities and registered partnerships:

1. Extract from the commercial register, which may not be older than six months; and
2. Evidence that the managers or persons responsible for managing TT Services are reliable.

c) to be submitted irrespective of the applicant’s legal form:

1. a description of the planned activities in accordance with (1);
2. Evidence of the minimum capital or a guarantee in accordance with Art. 13 (4c); and

3. Information on the TT Systems which are planned to be used, including a justification as to why the TT Service Provider assumes that the requirements of Art. 3 are met.

5) The application and the documents to be attached to the application may be electronically submitted to the FMA in accordance with the E-Government Act. If the FMA has any doubts regarding the authenticity of any of the attached documents, it may request that the applicant submits the original documents. In such a case, the document in question will not be deemed to have been received until it has been received in its original form.

6) Changes affecting the registration requirements must be reported to the FMA immediately. This notification to the FMA must be made prior to any public announcement.

7) If a financial intermediary already approved by the FMA wishes to provide one or more TT Services, the FMA may waive the documentary evidence requirements for registration in accordance with (4).

Art. 37
Registration

1) Based on the complete application and the information respectively documents submitted, the FMA must verify whether the registration requirements have been met. The FMA must make a decision regarding the complete application within three weeks and then, if the registration requirements are met, enter the applicant in the TT Service Provider Register in accordance with Art. 41. The FMA will notify the applicant of their entry in the system by sending

an extract from the TT Service Provider Register. The FMA may carry out registration subject to conditions and obligations.

2) If the registration requirements are not met, the FMA must establish this within the period specified in (1), notwithstanding a procedure according to Art. 48, and in the case of TT Services according Art. 36 (1), prohibit the exercise of the TT Service in question.

B. Cancellation

Art. 38
Expiration of Registration

1) Registration in accordance with Art. 36 (1) and (2) 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) the FMA revokes the registration in accordance with Art. 39;

e) bankruptcy proceedings are opened in respect of the TT Service Provider with legal effect; or

f) the company name of the TT Service Provider is removed 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 Art. 41.

Art. 39

Revocation of Registration

1) The FMA must revoke a registration in accordance with Art. 36 (1) and (2) if:

a) the registration requirements are no longer met;

b) the TT Service Provider obtained the registration by false information or the FMA was unaware of the essential circumstances;

c) a TT Service Provider systematically violates its legal obligations in a serious manner; 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 justified 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 Art. 41.

Art. 40

Consequence of the Cancellation of Registration

1) Upon cancellation of a registration of a TT Service Provider in accordance with Art. 36 (1), the TT Service Provider must immediately terminate the services provided for in the registration.

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.

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) In urgent cases the FMA may take the necessary measures without prior warning and without imposing a deadline.

C. TT Service Provider Register

Art. 41
Maintenance of the TT Service Provider Register

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

a) the TT Service Providers registered in Liechtenstein, citing the date of registration;

b) the extent of TT Services provided in accordance with Art. 36 (1) and (2);

c) any cancellation of a registration in accordance with Art. 38 or 39.

2) 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.

V. Supervision

A. General Information

Art. 42

Organisation and Implementation

The Financial Market Authority (FMA) is mandated with the implementation of this Act.

Art. 43

Official Secrecy

1) The authorities and bodies mandated to implement this Act, 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 other statutory provisions.

3) If bankruptcy or liquidation proceedings have been initiated over 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 specifically relate to the fulfilment of these tasks.. 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.

Art. 44
Cooperation Between National Authorities and Agencies.

The FMA and other competent domestic authorities and bodies shall work together to the extent necessary for the fulfilment of their duties.

Art. 45
Data Processing

1) The FMA and other competent domestic authorities and bodies may process personal data to the extent necessary for the fulfilment of their duties.

2) Authorities and bodies under (1) may disclose personal data to each other and to the competent authorities of another EEA member state or – under the requirements of data protection legislation – the authorities of a third state, insofar as this is necessary for the fulfilment of their tasks.

B. FMA

Art. 46
Responsibilities and Powers

1) The FMA is responsible for the following tasks:

a) The registration and cancellation of registrations;

b) Maintaining the TT Service Provider Register in accordance with Art. 41;

d) The prosecution of contraventions in accordance with Art. 49.

2) The FMA has all necessary authority to perform its tasks 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) in urgent cases, make all necessary arrangements, take all necessary measures, and issue all necessary orders without prior warning and without imposing a deadline.

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

4) If the FMA becomes aware of violations of this Act, ordinances issued in connection therewith, 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 as its observer to a TT Service Provider if the interests of users or creditors appear to be acutely endangered by mismanagement. The external audit office appointed 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 an activity subject to this Act is being conducted, the FMA may demand information and documents from the person concerned. In urgent cases, the FMA may order the immediate cessation and dissolution of the activity without prior warning and without imposing a deadline.

Art. 47
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

Art. 48

Proceedings and Legal Remedies

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

2) If a complete application for registration of a TT Service Provider is not decided within three weeks of its receipt, a complaint may be lodged with the FMA Complaints Commission.

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

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

VI. Penal Provisions

Art. 49

Contraventions

1) The FMA shall punish with a fine of up to CHF 30,000 for committing a contravention against TT Service Providers who:

a) have failed to register in accordance to Art. 36 (1);

b) use a designation contrary to Art. 23 which suggests an activity in accordance with Art. 36 (1);

c) fails to arrange for a regular audit or an audit required by the FMA;

d) fails to meet its obligations toward the external audit office;

h) fails to provide basic information or provide insufficient basic information in violation of Art. 28;

i) fails to comply with an decree or order issued to them by the FMA with reference to threat of punishment under this Article.

2) The FMA shall punish with a fine of up to CHF 20,000 for non-compliance if, contrary to Art. 36 (6a), a TT Service Provider fails completely, or in a timely manner, to notify the FMA.

3) The FMA shall impose fines on legal entities if the violations are committed by those legal entities within the ordinary course of business. Further, the FMA shall impose fines on other actors who have acted either alone; or as a member of the board of directors, management, executive board, or supervisory board of the legal entity; or on the basis of the actor's participation in another management position within the scope of the legal entity. The FMA:

a) is authorised to represent the legal entity externally:

b) exercise supervisory powers in a managerial capacity; or

c) otherwise exert significant influence on the management of the legal entity.

4) The legal entity will also be held responsible for contraventions committed by employees of the entity, albeit not culpable, if the infringement has been made possible or substantially facilitated by the fact that the persons named in (3) have failed to take the necessary and reasonable precautions to prevent such offences.

5) The legal entity’s responsibility for the offence and the criminal liability of the persons named in (3) or of employees in accordance with (4) for the same offence are not mutually exclusive. The FMA may refrain from punishing a natural person, where a fine has already been imposed on the legal entity for the same infringement and no special circumstances exist warranting the imposition of additional punishment.

6) When the offence is committed negligently, the maximum penalties set out in (1) and (2) shall be reduced by half.

Art. 50
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.

VII. Transitional and Final Clauses/Provisions

Art. 51
Transitional Provision

1) The provisions governing the issue of tokens (Art. 28-35) shall not apply if the tokens were offered to the public for the first time prior to the commencement of this Act.

2) The provisions on the disposal over tokens (Art. 6 -12) may retroactively be declared applicable to tokens generated before the commencement of this Act.

3) TT Service Providers, in accordance with Art. 36 (1), who started their activities prior to the commencement of this Act, must submit an application to the FMA for registration within six months.

Art. 53
Entry into Force

This Act shall enter into force on xxx 2019 subject to the unused expiry of the referendum period, otherwise on the day of its promulgation.

6.2 Amendment of the Due Diligence Act (SPG)

Law

from ...

on the amendment of the Due Diligence Act

I hereby grant My consent to the following Resolution adopted by the 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 Legal/Law Gazette. 2009 No. 47, in its current version, is amended as follows:

Art. 3
Scope of application

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

r) Token Issuers under the TT-Act (Trustworthy Technologies Act);

s) TT Protectors under the TT-Act;

t) Physical Validators under the TT-Act;

u) TT Depositaries under the TT-Act;

v) TT Identity Service Providers under the TT-Act;

w) TT Exchange Office Operators under the TT-Act;

Art. 23

Responsibilities

1) Responsibility for oversight and for the execution of this Act and the implementation of Regulation (EU) 2015/847 shall reside with:

a) the FMA with reference to persons subject to due diligence referred to in Art. 3 (1) a) to l) and n) to w);

II. Entry into Force

This Law shall enter into force at the same time as the TT-Act of #.#.####.

6.3 Amendment of the Financial Market Supervision Act (FMAG)

Law

from ...

on the Amendment of the Financial Market Supervision Act

I hereby grant My consent to the following Resolution adopted by the 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:

Art. 5

Functions

1) 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^{septies}) Law on Transaction Systems Based on Trustworthy Technologies (TT-Act, VTG);

Annex 1, Fee Rates

L. TT Service Providers

1. The fees for official processing within the framework of TT Service Provider registration under the TT-Act:

a) for the grant or refusal: 3000 Francs;

b) for the cancellation: 1,000 Francs;

c) for the expiration: 1,000 Francs.

2. The fees for the completion of other tasks in accordance with the TT-Act range from CHF 500 to 10,000, depending on the effort and complexity of the order being created.

Annex 2, Section VII. TT Service Provider according to TT-Act.

The annual supervisory tax for TT Service Providers is CHF 500.

II. Entry into Force

This law shall enter into force at the same time as the TT-Act of #.#.####.

6.4 Amendment of Persons and Companies Act.

Law

from ...

on the amendment of Persons and Companies Act.

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

I. Amendment of Existing Law

The Persons and Companies Act (PGR) of 20 January 1926, Liechtenstein Law Gazette. 1926. No. 004, in its current version, shall be amended as follows:

§ 81a (Final Part)

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 on uncertificated rights may also be

kept using Trustworthy Technologies in accordance with Art. 3 of the TT-Act (VTG) of xx.xx.2019.

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 rights in rem shall take place upon entry by the purchaser or the transferee in the ledger of uncertificated rights. If the ledger of uncertificated rights is kept using trustworthy technologies in accordance with Art. 3 TT-Act (VTG), its transfer or bailment shall be governed exclusively by the provisions of the TT-Act (VTG) from xx.xx.2019.

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-Act (VTG) of #.#.######.

6.5 Amendment of the Business Act (GewG).

Law

from ...

on the amendment of the Business Act

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

I. Amendment of Existing Law

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

Art. 3

Exceptions to the scope of application

s) Registered TT Service Providers in accordance with the TT-Act (VTG).

II. Entry into Force

This law shall enter into force at the same time as the TT-Act of #.#.####.