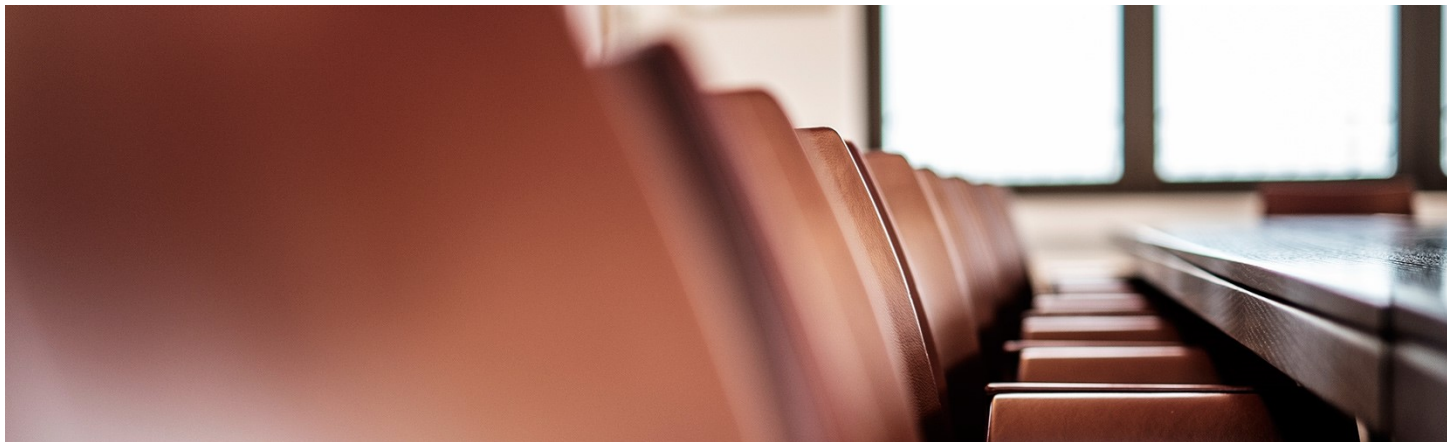**ELVINGER HOSS**

LUXEMBOURG LAW

« Tokenisation »: Which legal considerations should I have in mind and how should I amend my constitutional documents before issuing tokens?
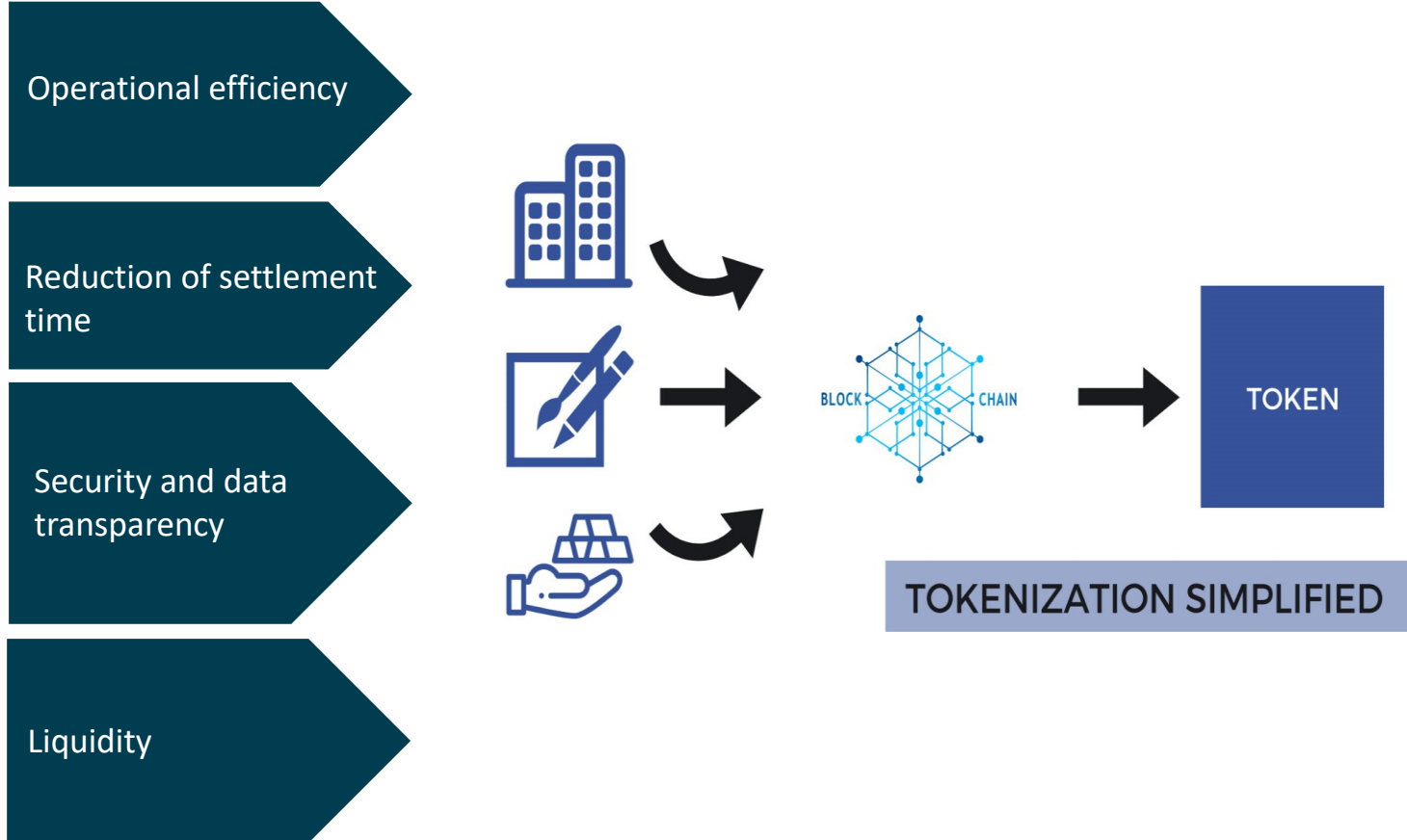
23 November 2020

Content

1. Introduction

2. Legal considerations prior to issuance

3. Legal considerations at the time of issuance

4. How should I amend my constitutional documents

5. European proposals of regulation: MiCA and DLT Pilot Regime

6. Conclusion

7. Questions?

1. Introduction

Why tokenising securities?

Operational efficiency

Reduction of settlement time

Security and data transparency

Liquidity

BLOCK CHAIN

TOKEN

TOKENIZATION SIMPLIFIED

The scope of the term « tokenised securities »

What are "tokenised securities"?

➢ traditional securities (equity or debt) wrapped into a token (i.e. both securities and tokens are issued)

➢ Traded via the tokens over a DLT

What are not "tokenised securities"?

➢ "*security tokens*" – new asset class embedding multiple rights similar to those of securities (i.e. only tokens are issued)

➢ "*utility token*" – meant to give access to services developed by the issuer of the tokens

➢ "*asset-referenced tokens*" – aim to maintain a stable value by referring to the value of fiat currencies, commodities or crypto-assets

➢ "*electronic money tokens*" – aim to maintain stable value by referring to the value of a fiat currency only

ELVINGER HOSS PRUSSEN

Which securities can be tokenised? (1)

BEARER SECURITIES

Form

- Securities issued in paper form
- Holder of the physical certificate is the rightful owner of such securities

Deposit

- Since the law of 28 July 2014 the bearer shares must be deposited with a depositary established in Luxembourg

Tokenisation

- Theoretically possible to tokenise the bearer shares once deposited, depending on whom is the depositary
- However, the intrinsic nature of the bearer securities practically excludes them from the tokenisation process

Which securities can be tokenised? (2)

DEMATERIALISED SECURITIES

Legal framework

- **Law of 6 April 2013** on dematerialised securities, as amended (the "**2013 Law**"): dematerialised securities are registered by way of inscription in an account specifically opened by the issuer maintained by a settlement organisation or an account keeper
- **1 March 2019**: a new article 18bis was inserted in the law of 1 August 2001 on the circulation of securities, as amended (the "**2001 Law**") stating that account keepers may hold **securities accounts** and register securities within or through secure electronic registration devices, including distributed ledgers or databases
- **Bill of Law 7637** was presented to Parliament with the key objective to expressly recognise the possibility to issue and record dematerialised securities on **issuance accounts** maintained through distributed electronic registers or databases

Tokenisation

- Possible to rely on the DLT for maintaining both securities accounts and issuance accounts – particularly relevant for securities to be issued by investment funds

Which securities can be tokenised? (3)

REGISTERED SECURITES

Form	• Represented by an inscription in a register of shareholders or bondholders
Register's requirements	• Legal requirements to maintain a physical register at the registered office of the company: 　• article 430-3 and 430-4 of the law of 10 August 1915 on commercial companies, as amended (the "**1915 Law**") for **S.A**; 　• article 710-8 of the 1915 Law for **S.à r.l**; 　• article 310-1(5) and 320-1(6) of the 1915 Law for **SCS** and **SCSp**; and 　• article 470-1 for the register of **bondholders** • Can be maintained in electronic format despite the express reference to the registered office in the 1915 Law • Information of electronic registers may be stored on different servers but must be readily accessible at the registered office of the company upon request
Tokenisation	• Analysis made in respect of registers in electronic format should be transposable to registers maintained using DLT • Legally possible to tokenise registered securities while being compliant with the 1915 Law

2. Legal considerations prior to issuance

Setting up a tailor-made smart contract (1)

Importance of "smart contracts"?

- Tokens are created through smart contracts and cannot be operated without a smart contract
- **What is a token**? A token corresponds to a unit entered into on the balance column of the blockchain register next to the blockchain address of a holder
- The smart contract governs all the actions that can be taken in respect of the tokens (issuance, transfer, cancellation, etc...)

Holder address	Balance
0x0000...0000	0
0x1f59...3492	100
0x2299...3ab7	100
0x4ba5...ae22	100
0x4919...413d	100
0x93f1...1b09	100
0xd8f0...c028	100
0xe20b...93b6	100
Total supply	700

Holder address	Balance
0x0000...0000	0
0x1f59...3492	110
0x2299...3ab7	90
0x4ba5...ae22	100
0x4919...413d	100
0x93f1...1b09	100
0xd8f0...c028	100
0xe20b...93b6	100
Total supply	700

Holder address	Balance
0x0000...0000	0
0x1f59...3492	110
0x2299...3ab7	90
0x4ba5...ae22	200
0x4919...413d	100
0x93f1...1b09	100
0xd8f0...c028	100
0xe20b...93b6	100
Total supply	800

Setting up a tailor-made smart contract (2)

What are smart contracts from a legal perspective?

- Smart contracts are in essence computer programs and not contracts in the legal sense
- Absence of definition of smart contracts under Luxembourg law and at European level
- Existence of **numerous computer codes and numerous blockchain** (Bitcoin, Ethereum, Stellar, etc…) renders their regulation difficult
- Existence of **different standards** of smart contract with different functionalities within the same blockchain

```
interface ERC777Token {
    function name() external view returns (string memory);
    function symbol() external view returns (string memory);
    function totalSupply() external view returns (uint256);
    function balanceOf(address holder) external view returns (uint256);
    function granularity() external view returns (uint256);

    function defaultOperators() external view returns (address[] memory);
    function isOperatorFor(
        address operator,
        address holder
    ) external view returns (bool);
    function authorizeOperator(address operator) external;
    function revokeOperator(address operator) external;
```

Setting up a tailor-made smart contract (3)

What are the key elements to be reflected and transposed in the smart contracts?

- Terms and conditions of the tokenised securities to be transposed in computer language
- Examples of smart contracts' features which need to be considered from a legal perspective:
  - ❖ total supply of tokens, which shall match the aggregate amount of tokenised securities issued (assuming a ratio 1:1)
  - ❖ issuance of new tokens ("**minting**" function)
  - ❖ redemption and cancellation of existing tokens ("**burning**" function)
  - ❖ mandatory transfers in case of a seizure by a regulator or authorised agent for example ("**killswitch**" function)
  - ❖ suspension of execution of transactions on the blockchain, for example in case of hard fork ("**freeze**" function)

`Minted` **event**

```
event Minted(
    address indexed operator,
    address indexed to,
    uint256 amount,
    bytes data,
    bytes operatorData
)
```

Indicate the minting of `amount` of tokens to the `to` address by the `operator` address.

NOTE: This event MUST NOT be emitted outside of a mint process.

parameters
- *operator* : Address which triggered the mint.
- *to* : Recipient of the tokens.
- *amount* : Number of tokens minted.
- *data* : Information provided for the recipient.
- *operatorData* : Information provided by the operator.

`Burned` **event**

```
event Burned(
    ddress indexed operator,
    address indexed from,
    uint256 amount,
    bytes data,
    bytes operatorData
);
```

Indicate the burning of `amount` of tokens from the `from` address by the `operator` address.

*NOTE*: This event MUST NOT be emitted outside of a burn process.

parameters
- *operator* : Address which triggered the burn.
- *from* : Holder whose tokens were burned.
- *amount* : Number of tokens burned.
- *data* : Information provided by the holder.
- *operatorData* : Information provided by the operator.

Setting up a tailor-made smart contract (4)

How the smart contract is put in place?

- Smart contracts are deployed on the relevant blockchain once their terms and conditions have been agreed
- New transaction entered into on the relevant blockchain, which must be validated by its participants
- Tokens are assigned to the blockchain addresses (or public keys) of the subscribing investors by the issuer, generally at the end of the offer period
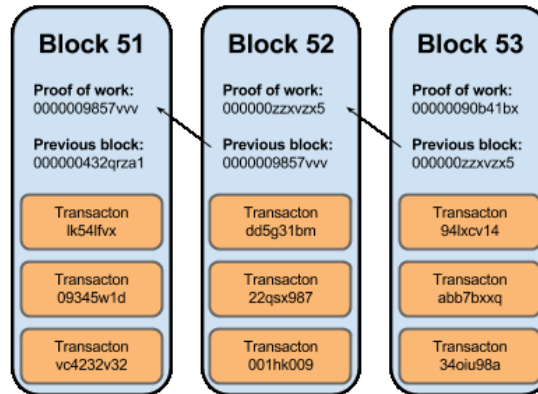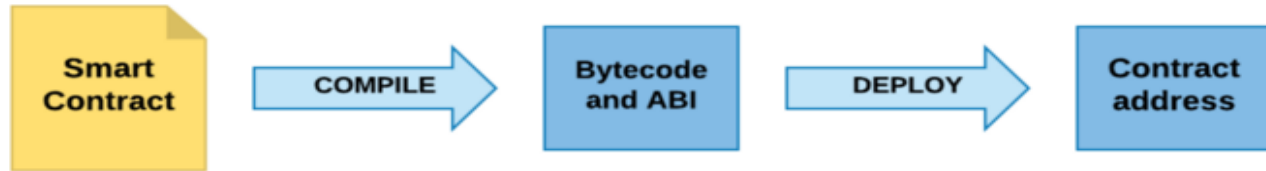
Servicing agreement (1)

What is the role of a "default operator"?

- Either the issuer of the tokenised securities or an entity appointed by the issuer and acting on its behalf (the "**Servicer**")

- It has considerable powers as it is effectively the "owner" of the smart contract

- Person able to interact with the tokens

- Person able to activate functions such as *minting, burning or freezing* of tokens

What is the importance of the servicing agreement?

- Established if the issuer of the tokenised securities lacks the adequate personnel, blockchain expertise and/or infrastructure to manage the tokenisation process (e.g. a SPV issuing tokenised securities)

- Servicing agreement governs the relationship between the issuer and the Servicer which will administer the platform and manage the tokens from a technical perspective

Servicing agreement (2)

Examples of services to be covered by the servicing agreement

➢ **On-boarding services:**

  ❖ Collection of KYC/AML information and verification of the source of funds

  ❖ Validation and verification of the status of the investors (i.e. qualify as professional clients)

  ❖ Collection of subscription forms and payments from investors

➢ **Services related to the smart contract and the platform**

  ❖ Set-up of the smart contract and its deployment on the relevant DLT

  ❖ Custody of the private key associated to the issuer' smart contract

  ❖ Allocation of the tokens to the DLT addresses of the subscribers

  ❖ Maintenance of the platform and ensuring its accessibility on a continuous basis

➢ **Information exchange between the issuer and the Servicer**

  ❖ Set-up of a system of an information flow and checks and balances, in particular in respect of any transfer of tokens or in case of specific events affecting the tokens (e.g. hard fork)

  ❖ Interface to transcribe encrypted data on blockchain into plain language for the benefit of the default operator, the issuer, the domiciliation agent, etc…

3. Legal considerations at the time of issuance

Scope of the offer of tokenised securities

Offers within the scope of the Prospectus Regulation

- For offers of tokenised securities to the public, Regulation (EU) 2017/1129 (the "**Prospectus Regulation**") applies:
  - ❖ Issuers should keep in mind that the drawing up of a prospectus will entail compliance with all ESMA guidelines, including in particular as regards the risk factor section of the prospectus

Offers pursuant to an exemption to the Prospectus Regulation

- Offers of tokenised securities can be made within an exemption to the Prospectus Regulation:
  - ❖ Offer by way of private placements (150 natural or legal persons per member state), offer to qualified investors or offer whose denomination per security exceeds EUR 100,000
  - ❖ Other exemptions exist: (i) offer of less than EUR 1 million within the EU over a 12-month period or (ii) offer of less than EUR 8 million within the EU over a 12-month period (with a notification to the CSSF required for offers ranging between EUR 5 million and EUR 8 million)

Offering document (1)

What type of offering document?

- If the offer of tokenised securities is made within one of the exemptions, no prospectus will have to be drawn up but an offering document (PPM or subscription agreement) is still advisable, with DLT specificities to be addressed in the terms and conditions and risk factor sections

Risk factors: which risks should be brought to the attention of investors?

Risks associated with the smart contract

- Tokens are generated through the issuer' smart contract which may be subject to bugs, coding errors or cyber attacks: investors should be aware of the risk that the smart contract may cease to operate and impairs their rights
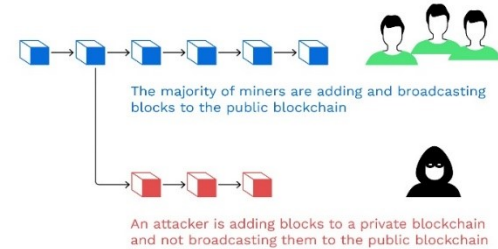

Technological risks

- Most of the DLTs used being public (e.g. Ethereum, Bitcoin), they are subject to technological risks which need to be explained to investors as they may affect their tokens:
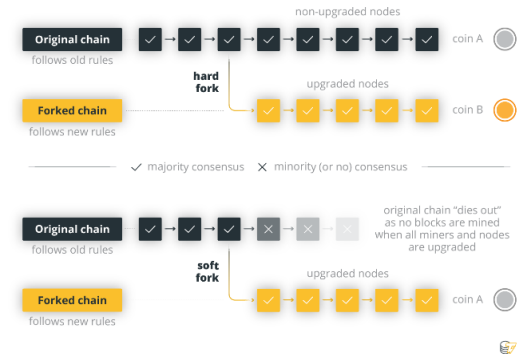
Offering document (2)

❖ **51% attack**? Occurs when one miner or a pool of miners controls more than 50% of the computing power of the network and can therefore interfere with the validation of new blocks and obtain all the rewards for such validation

❖ **Distributed denial of service**? Consists in disrupting the network by overloading the traffic on the network from multiple sources which leads to malfunctions and may block the entire network, thus preventing any transaction to occur

❖ **Hard fork**? Occurs when the source code of the DLT is changed and only part of the participants/nodes of the network download the update which leads to two chains of blocks. This risk can be anticipated by issuers with additional provisions inserted in the constitutional documents

What is a 51% attack?

The majority of miners are adding and broadcasting blocks to the public blockchain

An attacker is adding blocks to a private blockchain and not broadcasting them to the public blockchain

What are hard and soft forks?

non-upgraded nodes

Original chain
follows old rules — coin A

hard fork — upgraded nodes

Forked chain
follows new rules — coin B

✓ majority consensus   ✗ minority (or no) consensus

Original chain
follows old rules — original chain "dies out" as no blocks are mined when all miners and nodes are upgraded

soft fork — upgraded nodes

Forked chain
follows new rules — coin A

Offering document (3)

## Risks associated with the use of wallets and private keys

- **What is a wallet and a private key**? DLT relies on asymmetric cryptography which means that transactions are entered on DLT through a public key (known to the entire network) and a private key (specific to each user) which permits to encrypt and decrypt data. Public and private keys are stored on wallets generally maintained by wallet service providers which ensure their safe custody
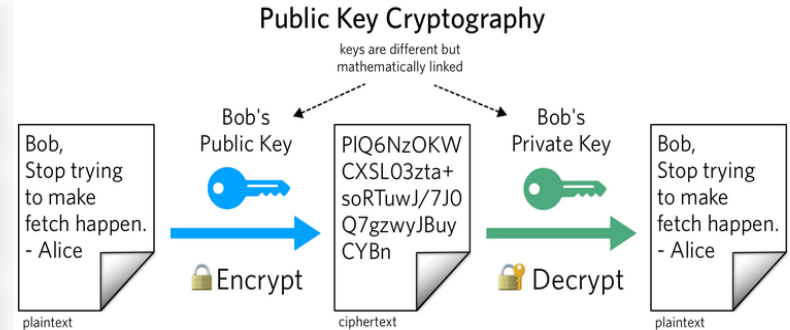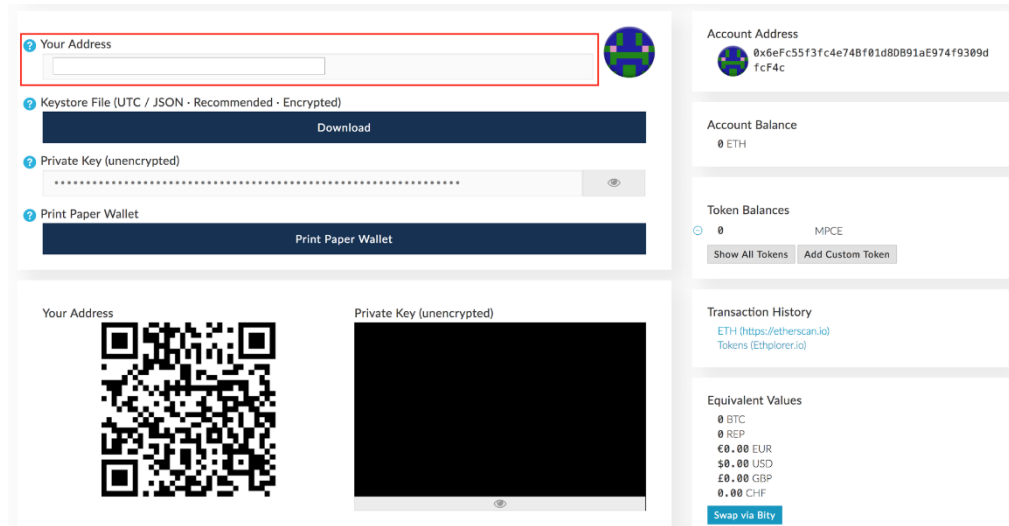
Offering document (4)

- **What are the risks**? A user can **lose his private key** which would prevent the user to enter any transaction on blockchain or the **private key may be stolen** due for example to a cyber attack or a malicious virus targeting the wallet software
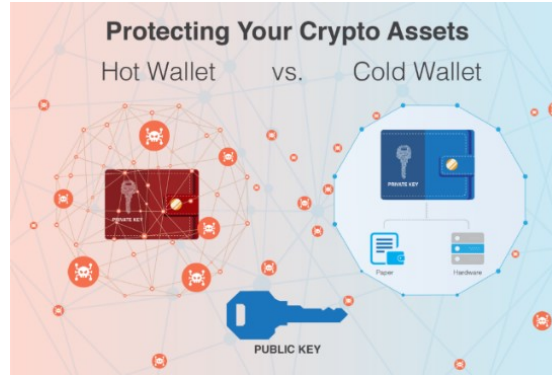
- **How to remedy these risks**? Specific procedures inserted in the constitutional documents. These risks must be clearly set out in the offering document and if the constitutional documents are not amended, then express provisions should be included in the terms and conditions of the tokenised securities

Legal and regulatory risks

- These risks are particularly relevant in the current context given the European proposals which will in the future impact the regulation of crypto-assets

Offering document (5)

Terms and conditions: which DLT-specific terms need to be included ?

How many tokens do I get in exchange of one security?

- Ratio securities/token (generally, the ratio is 1:1)

How do I subscribe to tokenised securities?

- Wallet compatible with the issuer' smart contract
- On-boarding process
- Fill out the relevant subscription form
- Pay for such subscription

How and when do investors finally get assigned their tokens?

- At the end of the offer period

Offering document (6)

Register on Blockchain

- Register or ledger on blockchain (where the tokens are registered) consists of encrypted data
- It must be reconciled with the register required under Luxembourg law and the terms and conditions need to explain how this is achieved.
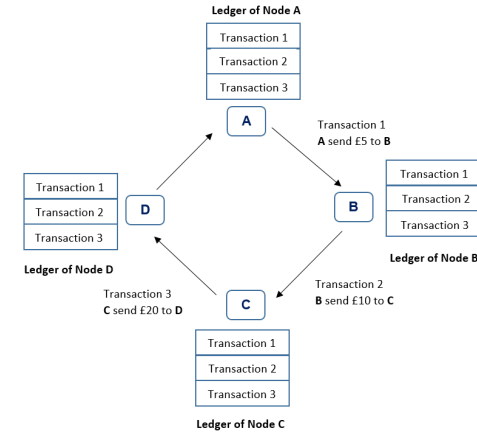

- The register on blockchain will recognise as holder of tokens the person whose blockchain address is assigned to such tokens

Offering document (7)

- How to comply with the 1915 Law?
  - ❖ **Issuer is a node** (i.e. a participant) of the network and in such capacity has a copy of the blockchain register and through an interface of the smart contract (as well as the information collected at the time of the on-boarding) can transcribe the encrypted data into the required information in the register
  - ❖ Issuer creates an **electronic register which mirrors the blockchain register**
- In both cases, the smart contract must include the interface mentioned and the servicing agreement needs to clearly set out the role of the Servicer vis-à-vis the issuer for sharing information in relation to the blockchain register and transfers occurring on that register

Ledger of Node A

| Transaction 1 |
| Transaction 2 |
| Transaction 3 |

A

Transaction 1
A send £5 to **B**

| Transaction 1 |
| Transaction 2 |
| Transaction 3 |

D

B

| Transaction 1 |
| Transaction 2 |
| Transaction 3 |

Ledger of Node D

Ledger of Node B

Transaction 3
C send £20 to **D**

C

Transaction 2
B send £10 to **C**

| Transaction 1 |
| Transaction 2 |
| Transaction 3 |

Ledger of Node C

4. How should I amend my constitutional document?

How should I amend my constitutional documents? (1)

No legal obligation to amend the constitutional documents before issuing tokenised securities but it is recommended to do so:

- to anticipate DLT-specific issues that may arise and affect the rights of tokenholders
- to render such provision easily enforceable vis-à-vis third parties

How to protect the rights of tokenholders if their tokens are lost or stolen?

- Occurs when a holder of tokenised securities is no longer in control of his private key and can therefore not transfer or manage his tokens
- **Private key is lost** – constitutional documents may provide for a specific procedure to resolve this issue, similar to the following one:
  - ❖ Notification of the issuer of such loss and indication of the blockchain address to which the tokens are assigned
  - ❖ Verification by the issuer and decision to cancel ("*burn*") and re-issue ("*mint*") the tokens to a new blockchain address to be provided by the person who lost the private key
  - ❖ All rights attached to such tokenised securities are suspended until the lost tokens have been re-issued

How should I amend my constitutional documents? (2)

Example of clause for lost tokens

"*In case of registration of [Tokenised Securities] in the Register of Bondholders or in the Register of Shareholders, as applicable, and if a holder of Tokenised Securities (the "**Applicant**") has lost access to the tokens associated with such Tokenised Securities (the "**Lost Tokens**"), such Applicant shall as soon as practicable notify the Company of such loss and specify his/her/its Ethereum Blockchain's address (or any other equivalent address of any other distributed ledger technology determined by the Company).*

Upon receipt of such notification, the Company shall verify the identity of the Applicant to ensure that he/she/it is the rightful owner of the Lost Tokens. On completion of that verification, if the Applicant is identified by the Company as the rightful owner of the Lost Tokens, such Lost Tokens shall be cancelled ("burnt") and re-issued ("minted") to a new Ethereum Blockchain's address (or any other equivalent address of any other distributed ledger technology determined by the Company) designated by the Applicant."

How should I amend my constitutional document? (3)

- **Private key is stolen** – procedure similar to the one for lost tokens with one additional step necessary in order to determine who is the rightful owner of the tokens:

  ❖ Publication of a notice stating that unless a person can provide evidence of his ownership of the tokens, the tokens that have been stolen will be cancelled ("*burnt*") and re-issued ("*minted*")

  ❖ If no third party is able to provide such evidence, the tokens will be re-issued to a new blockchain address provided by the person who first notified the issuer

- If these provisions are not included in the constitutional documents, it is crucial to include them in the offering documentation

How to prepare for a hard fork?

- It is recommended to expressly give authority to the board to decide which version of the blockchain should be retained and to activate the "freeze function" on the smart contract to protect the rights of tokenholders

> "*In case of split of the Ethereum Blockchain (or any other distributed ledger technology determined by the Company) resulting in two separate chains of blocks, the Board shall be responsible for determining which version shall be retained and for taking all the necessary steps to protect the holders of Tokenised Securities*".

How should I amend my constitutional documents? (4)

How can I ensure that the securities will remain in registered form?

- Exclusion of the application of article 430-8 of the 1915 Law (which provides for such conversion) in the constitutional documents

Who is responsible for the tokenisation process?

- Competence of the board should be indicated in the constitutional documents to avoid any possible legal discussions as to whom is competent between the board and the general meeting
- Board will be competent in particular to determine the conditions of issuance, the features of the smart contract and the conditions for the transfer and registration of tokenised securities
- **Example of clause**:

> "*In the event of tokenisation of shares, the Company shall identify the holders of the tokens associated with the relevant shares in order to record them in the Register of Shareholders of the Company. The Board shall determine the methods of identification of such holders of Tokenised Shares which shall be similar to the information for the [Registration Request] of a new holder of Tokenised Shares. Such methods may be automated through the use of any electronic means at the discretion of the Board*".

How should I amend my constitutional document? (5)

Which information needs to be collected to register a holder of tokenised securities?

- Not necessary to detail the whole identification procedure in the constitutional documents but delegation to the board to establish such procedure should be expressly given

- **Information to be provided** ? Blockchain address (i.e. public key), personal information (name, place of residence or registered office, nationality) and confirmation that the holder is not a nominee

- Information generally collected at the time of the on-boarding process

5. European proposals of regulation: MiCA and the DLT Pilot Regime

Traditional classification of tokens

- Prior to the publication of MiCA, most authors and regulators were classifying the tokens in 3 main categories:

  ❖ **Investment-type tokens (i.e. security tokens)** – same characteristics as securities i.e. (i) issued in standard form (i.e. belonging to the same class), (ii) negotiable on the capital markets and (iii) having the same characteristics as shares, bonds or securities giving right to acquire shares or bonds (excluding the instruments of payments)

  ❖ **Utility-type tokens** – give access to services developed by the issuer of the tokens and which function in a similar way as vouchers or pre-paid cards

  ❖ **Payment-type tokens** – constitute a means of exchange that can be used in relation to services or goods offered by the issuer

- In practice, tokens often have a hybrid form which means that a case-by-case analysis is generally recommended to determine their legal qualification
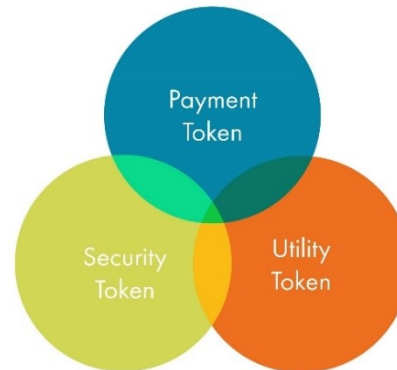
Classification of tokens under MiCA

Overview of the European proposals of regulation

- European Commission published on 24 September 2020, a proposal for a regulation on markets in crypto-assets ("**MiCA**") and a proposal for a regulation on a pilot regime for market infrastructure based on DLT ("**DLT Pilot Regime**")

- Pragmatic approach taken by the European Commission

- **Crypto assets** are defined as "*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology*"

- Are excluded from the scope of MiCA, crypto-assets which qualify (i) as "financial instruments" within the meaning of MiFID and (ii) as "electronic money" as defined in Directive 2009/110/EC

    - ➢ tokens qualifying as financial instruments (i.e. security tokens) shall be regulated as financial instruments in accordance with the existing European financial regulations (Prospectus Regulation, MiFID, etc...)

    - ➢ tokens qualifying as electronic money (i.e. payment tokens) shall be regulated in accordance with Directive 2009/110/EC

Classification of tokens under MiCA (2)

Which tokens fall under the scope of MiCA?

Utility tokens

- Offers to the public of utility tokens require the publication of a white paper (article 5 of MiCA)
  - ❖ **Exemptions** exist for example if utility tokens are (i) offered for free, (ii) automatically created through mining as a reward or (iii) unique and not fungible with other crypto-assets

Asset-referenced tokens

- This is the first form of the so-called stablecoins
  - ❖ **What is a stablecoin**? It is a crypto-asset which purports to maintain a stable value by referring to an underlying asset. Stablecoins have a payment function and may serve as a store of value
  - ❖ **What is the scope of asset-referenced tokens**? Broader than for electronic money tokens as the underlying asset can be several fiat currencies, one or several commodities or one or several crypto-assets
- Offers to the public of asset-referenced tokens require the publication of a white paper (article 17 of MiCA)

Electronic money tokens

- This is the second form of stablecoins
  - ❖ Scope is narrower than the asset-referenced tokens as their value is determined solely by referring to one fiat currency
  - ❖ Offers to the public of electronic money tokens also require the publication of a white paper (article 46 of MiCA)

DLT Pilot Regime

- The DLT Pilot Regime aims at regulating financial instruments that are traded on DLT market infrastructures (i.e. DLT multilateral trading facility or DLT securities settlement system)

- The DLT Pilot Regime introduces the concept of DLT transferable securities which are transferable securities in the sense of MiFID which are "*issued, recorded, transferred and stored using DLT*"

- **Limited scope**: it will only apply to DLT transferable securities traded on a DLT market infrastructures

- The DLT Pilot Regime will complement the amendments already made by the Luxembourg legislator in the 2001 Law and to the 2013 Law (assuming Bill of Law 7637 will eventually be voted by Parliament)

6. Conclusion

Conclusion

➢ There is currently no clear legislative framework regulating the issuance of tokens under Luxembourg law but it is possible to issue tokenised securities

➢ Pre-issuance steps are important (i) to align the computer code of the tokens (i.e. the smart contract) with the conditions of the tokenised securities (set out in the offering document) and (ii) to determine the role and responsibilities of the Servicer which will operate the tokens from a technical perspective

➢ The risk factor section and the terms and conditions of the tokenised securities must include all the DLT-specific provisions introduced in this presentation

➢ Important to amend the constitutional documents to anticipate certain events that may affect the rights of tokenholders such as a hard fork or the case where tokens are lost or stolen. The benefit of doing so is that it permits to easily enforce such provisions vis-à-vis third parties

➢ With MiCA and the DLT Pilot Regime, the regulation of crypto-assets will continue to evolve in the near future

7. Questions

KARL PARDAENS
Partner

karlpardaens@elvingerhoss.lu
Tel: +352 44 66 44 5368

Contact us to discuss how we can support
your business in Luxembourg

Luxembourg Office
2 Place Winston Churchill
L-1340 Luxembourg
Tel: +352 44 66 440
Fax: +352 44 22 55
www.elvingerhoss.lu

Hong Kong Office
Suite 503, 5/F ICBC Tower
Three Garden Road, Central
Hong Kong
Tel: +852 2287 1900
Fax: +852 2287 1988