# ERASMUS + Chaise Project - Module 2: Regulation, Legal aspects and Governance of Blockchain systems Lecture 4: Blockchain regulation

Frédérique Biennier

# Module 2: Regulation, legal aspects and governance of Blockchain systems

## Lecture 4: Blockchain regulation

**Frédérique BIENNIER**

Univ Lyon, INSA Lyon, CNRS, UCBL, Centrale Lyon, Univ Lyon 2, LIRIS, UMR5205, F-69621 Villeurbanne, France

# TABLE OF CONTENTS

# 1 INTRODUCTORY PARAGRAPH

In this second module, we focus on the way blockchains are governed and regulated. In this fourth lecture, we focus on blockchain regulation, i.e. identify the blockchain actors and the way their interaction with their environment is legally controlled. This lecture takes advantage of the knowledge provided in the previous lectures, i.e. defining the blockchain context (lecture 1), the governance background (lecture 2) and the organisation of the blockchain ecosystem (lecture 3).

Identifying blockchain regulation principles, existing legal frameworks… involves identifying the regulation scope. Should Blockchain regulation be focused on the technology or on blockchain deployment and usages? To define the regulation perimeter, we have first to identify regulation motivations / main requirements. As a technologic object, blockchain systems are deployed on the Internet, should regulation depend on existing boarders or is there any worldwide regulation? Are there specific requirements related to the blockchain systems or can blockchain regulation be derived from other regulations? Are there some usage dependent regulations? Why?

All these questions and their answers are not so simple. Let's think and brain storm regarding these questions

As you can notice, describing blockchain regulation requirements and challenges is not so simple. This requires identifying key regulation principles, i.e. understanding why and how regulations are set, understanding the regulation context. This lecture is designed to provide the necessary knowledge to understand and discuss key regulation principles, blockchain regulation requirements. To understand and discuss the way regulation mechanisms are applied to the blockchain context, you will be introduced to the virtual asset protection context before learning the way applicable regulation mechanisms are applied to blockchain usages.

To sum up, this lecture addresses different learning objectives:

1. Regulation context: focusing on the blockchain context, you will learn the basic regulation motivation by identifying what needs to be regulated, i.e. either the core technology or the usages relying on this technology. This will guide the identification of the key blockchain regulation challenges.
2. Blockchain key regulation principles: based on motivations and challenges for blockchain regulation, you will learn how regulation incentives are set to support blockchain development and key technic regulation principles such as the blockchain "legal status" and the way it has been designed, smart contract status… As Blockchain 1.0 is mostly associated to Fintech and virtual assets, we pay a particular attention on the way regulation impacts the token status and the way Fiat currencies are legally defined.
3. Virtual assets regulation: Considering blockchain as a support for virtual assets development, you will be introduced to virtual asset regulation motivations, mostly introduced to face specific risks. You will also get knowledge on international regulations implementing the propositions of the Financial Action Task Force, in inter-governmental organisation founded in the late 80s by the G7, in charge of proposing policies to control money laundering and terrorism financing (Transfer of Fund Regulation and Market in Crypto-Assets Regulation).

# 2 LECTURE NOTES

According to the learning objectives, this lecture is organised into three main parts. We will first introduce the regulation context, introducing technology regulation challenges and detailing key blockchain regulation challenges based on the blockchain typology. Based on these regulation motivations and requirements, we expose then the blockchain key regulation principles. This part will introduce the main blockchain incentives and the blockchain legal status before focusing on token status and fiat currencies regulation key principles. As the blockchain is largely used to support FinTech and crypto-currency development, the last part of the lecture will present regulation motivation and key risks associated to these virtual assets before introducing regulations derived from the Financial Active Task Force, an intergovernmental organisation in charge of fighting money laundering and terrorism financing.

## 2.1 Regulation context

### 2.1.1 Technology regulation

First of all, let's come back to basis, defining precisely what regulation means. As introduced in previous lectures, regulation control the interactions of an ecosystem with its environment. Regulation is defined (according to Cambridge or Collins dictionaries) as an official rule or act or as the action of checking whether a business follows or not the official laws, social rules... Focusing on the regulation rules, acts, laws and even social rules are defined by authorities either governments or recognized authorities. Their design follows specific validation process before being submitted formally for approval. Once approved, these acts / laws are promulgated. We can note that laws can be either primary or secondary laws. A secondary law amends an existing law, may add rules or precise law application context and rules. In other words, the secondary law "derives" and amends rules from a primary law. In an evolving context, it means that the primary law provides the global scope and secondary laws are used to precise it.

As regulation laws and acts are defined by each country, it means that rules may be different from one country to another. This leads to key questions to identify which laws are applicable and which court has jurisdiction and it involves that laws must include territoriality / extraterritoriality explicit conditions. Law territoriality means that the law is applicable depending on the physical place where the actions take place. Law extra-territoriality means that a jurisdiction of a country can be competent according to some conditions even if the action does not occur physically in the country. For example, GDPR provides an extra-territorial personal data protection for EU citizens.

Focusing on Business regulation, common worldwide rules are defined. First of all, business interactions are supported by contracts. Contracts gather a description of the business interaction, applicable rules… Contracts are written in the style of a law and contains several articles. They usually include:

- The precise identification of the different parties, i.e. the party verified identity, its role / responsibility used to refer to it in the contract and who will represent this party to approve the contract

- The business purpose, i.e. the exact definition of what will be done / provided by which party to achieve a precise goal.
- The applicable business rules, i.e. rules related to extra requirements including the time validity / time constraints, quality related rules such as required quality measures, responsibility and pricing for each party, contract execution conditions, who will be responsible of what…
- The applicable legal environment i.e. the competent jurisdiction accepted by all parties in case of troubles means that all parties accept that the applicable laws are the ones from the country of the accepted jurisdiction.

Contracts must be approved by all parties who have to sign them to authenticate them. Several copies of the contracts are signed so that each party has its own originally certificated copy of the approved contract. A party can use its own copy to "prove" that the contract has been approved.

Blockchain technology can be integrated in this contract approval process. By providing a trusted certification and a trusted storage, contracts can be stored immutably in the blockchain. Nevertheless, as Blockchain supports only P2P transactions, a dedicated approval process must be set to support the automated signature protocol. Moreover, depending on the type of blockchain (permissioned or permissionless) a particular attention must be paid on confidentiality constraints: contracts must be encrypted so that they cannot be read by unauthorized parties and trade secrets are protected.

When blockchain is used to support business development and interactions between parties, a particular attention must be paid on the type of blockchain, i.e. public blockchains which are ready-to-use and require reduced investment or consortium/private blockchains which require investments and more time to be deployed. Depending on the type of blockchain, of its ecosystem… different legal framework may apply and it will impact the business regulation.

What we just said means that technology or its usage may impact business regulation. As a consequence, technology or its usage needs to fulfil regulation rules. In fact, technology can be considered as an "inert" passive object. Its implementation allows using it and the way t interacts with its environment depends on the usage. So it is rather the way the technology is developed, implemented and used that requires regulation. Technology, its design and its usage must comply their legal environment. This legal compliance requirement covers core development (developing a technology must comply ethic, economic, environmental, security, business… regulations) as well as usage development as implementing and using the (new) technology may have social, economic and environmental impacts.

To sum up technology is regulated to ensure that its impacts comply with the law.

As technology can be used worldwide, regulation territoriality must be considered. In fact, different usages can be allowed or forbidden depending on countries. As far as "tangible" technologic objects are considered, identifying the convenient legal framework depends on the place the object is physically located and used. For non-tangible technologic objects, there's no worldwide regulation: a particular attention must be paid on the "usage location", on the location of the technology owner and where the usage support system is physically located.

As an innovative technology, we have to evaluate requirements paying attention to the way the technology is designed and implemented as well as the requirements associated to the usage socio-economic context and impacts.

### 2.1.2 Blockchain regulation requirements and challenges

Focusing on the technologic side, Blockchain provides a trusted P2P transaction support. The secured immutable storage of transactions into blocks proves that the transaction occurs. It means that peers delegate the double-spending problem proof to the blockchain. The integration of block and tokens history "on-chain" allows developing ad-hoc "backtracking" processes to fit legal tracking requirements.

Paying attention to the intrinsic cryptographic functions used to authenticate blocks, different regulations may be applied depending on countries. Data encryption can be seen as a major security risk for a state and there may be specific regulations limiting the usage of cryptographic algorithms. These regulations may affect any data hosted or transmitted in the country as well as any data used by any people from this country. Another point to consider is that cryptography is used as the basis of users' authentication. A user is simply associated to a cryptographic key. By signing transactions, it means that the transaction is approved by the entity owning the private key. There's no proved association between this "cryptographic-based identity" and the real identity. In other words, a transaction can be attached to a cryptographic identity BUT not to a real identity.

As a distributed architecture, blockchain regulation is also motivated by accounting and responsibility limits related requirements. Of course, token exchanges are trackable as well as transactions but the blockchain immutability relies on the consensus mechanism. This leads to a co-responsibility of all actors involved in a blockchain as they share a common asset: the blockchain itself. As threats can focus on different entry points, it means that blockchain systems must comply security requirements as other IT systems and develop also specific risks analysis to cope with the intrinsic distributed organisation own risks.

Paying attention to the interactions a blockchain has with its environment, we can identify different impact categories that may motivate regulation:

1. A Blockchain is a distributed system that requires a distributed infrastructure. This physical infrastructure impacts mostly its environment due to the energy it consumes (IT and cooling systems…). As the energy transmission grid as limited capacity, data centres must anticipate their consumption to get appropriate authorisations (in other words, a data centre cannot grow up if it will lead to a black-out). These limitations must be taken into account while choosing physical location for blockchain nodes (specially for private blockchains).

2. Specific tokens are associated to the different blockchain ecosystems. These tokens may be utility tokens (i.e. "technical assets" allowing to use the blockchain system) or securities (as crypto-currencies). Security tokens are de facto unregulated fiat currencies, without any counterpart in the real world. Developing a new trans-national currency impacts the economy and must be regulated as other fund transfer systems. Consequently, different legal constraints must be taken into account depending on the token exact status

As a distributed and poorly interoperable system, blockchain ecosystem governance requires a particular attention. In order to protect the different stakeholders involved in a blockchain ecosystem, regulation may control the way blockchain is governed. In other words, as blockchain is a rather closed system, people investing in blockchain projects must take part in the blockchain decision and specific regulations may be applied to protect them and their investment.

From the early cryptographic techniques to the last blockchain 4.0 technology, we can identify different regulation challenges related to

1. State security and protection: Data encryption may appear as a threat for state security, but the main risk is related to the intrinsic fiat currency developed and owned by the blockchain. This fiat currency associated to the token, even if the token is a utility token as tokens are given as counterparts of the initial fundraising. As securities, tokens are associated to fund transfer and must comply fund transfer regulation as well as anti money laundry regulations.
2. Blockchain-based business development: it challenges to grant a legal status for the blockchain transactions, more specifically for smart contracts. As an IT system, blockchain must also comply rules associated to other IT systems: it must provide action accountability (including logs, transaction tracking) and the system must be consistently protected. The « immutability by design » promoted by the multiple replications and the trusted consensus process may face all threats. Felon stakeholders can corrupt the blockchain, taking advantage of the consensus process to hack the blockchain, steal tokens and rob blockchain users… This has already occurred for the DAO, leading members of the ecosystem to decide forking the blockchain
3. The development of Blockchain as a Service, the integration of IoT requires paying attention to personal data protection. As more and more personal data can be used, consumed, stored… blockchain system must comply with personal data regulation, namely GDPR.

## 2.2 Blockchain key regulation principles

As we've just seen there are several regulation challenges. We present now regulation principles dealing on one hand with the blockchain incentives and core technology and on the other hand with the token status and the fiat currency development.

### 2.2.1 Incentives and key technic regulation

First of all, regulating blockchain interaction with its environment encompass both incentives to develop blockchain technology and usages AND rules constraining the blockchain system operation and blockchain usages.

We can identify different kinds of incentives to support blockchain development:

1. Regarding blockchain infrastructure, taxes on energy supply can be used to regulate data centres development, allowing a smooth integration in their environment and supporting their potential development. The establishment of data centres has a strong economic interest in ensuring spatial planning: the development of this activity leads to the development of the associated territory, on one hand, because the necessary electricity and data networks are being set up, and on the other hand because of the jobs created.

2. Economic incentives can also be set to support “sovereign blockchains”, i.e. the “local” development of blockchain systems and products. Of course, this does not fit the “universal openness” of traditional public blockchains but setting sovereign blockchain allows securing further business developments by defining precisely the applicable legal framework, providing clear constraints on the location of the physical infrastructure so that data protection can be defined precisely. This can also bring some guaranties regarding Blockchain availability.

3. Regulation can also integrate incentives to promote technology development. Due to its novelty and to the potential usages’ novelty, it is not possible to fix a priori a strict regulation perimeter regarding blockchain evolution. Favoring innovation requires evaluating technologies and their usages before adapting / defining rules to regulate these new usages. Sandboxes provides environment to evaluate technology development and usages, paying attention to the impact it may have on its environment. After this evaluation phase, rules can be enacted more precisely to control this technology / usage consolidation.

So has blockchain a legal status? Blockchain technology was created in 2009, establishing the first crypto-currency (the Bitcoin). Then Ethereum establishing the first smart contract was launched in 2015. At fall 2015, the French law “Macron 2” has specified the first legal integration of Blockchain technology. In this law, dedicated to “new economic opportunities”, blockchain is considered as an innovative way to record (financial) transactions so that the existing rules must be adapted accordingly. Paying attention to business development, smart contracts appear as an efficient way to implement P2P contracts, leading to recognise these contracts as legal contracts. This leads to establish the first legal framework associated to blockchain, focusing mostly on mini-bonds registration (to favour technology development investments) and financial applications.

Then in 2017, the Arizona house defines more precisely the blockchain as a distributed ledger providing “theoretically” immutable data and providing an uncensored truth. This definition, which has served as a common base for the US federal blockchain regulation, provides constraints on the way blockchain systems are organised:

1. 1: cryptography used to protect data must be compliant with the current knowledge to ensure the theoretical data protection
2. 2: the system must provide an uncensored truth: this means that blockchain must be neutral, i.e. must protect every data in the same way. This constraint blockchain security and blockchain governance

Smart contract is defined as an automatically executed transaction. It is often presented as the automated execution of a real world contract linking parties, defining precisely the contract execution conditions and the contract purpose. Nevertheless there are some significative differences with traditional contracts:

1. As traditional IT transactions, a smart contract implements a P2P transaction. As such it cannot be set to implement multi-party contracts
2. The process that is automatically executed when the smart contract is “fired”, is a rather simple process that do not require other external inputs than those used to launch it.

Contracts and smart contracts are quite different. As a “legal object”, parties approving a contract must be clearly identified. Whereas the blockchain stores signed smart contract, the signature is related to a blockchain user which is not related to a “real and trusted physical identity”. This leads to a key challenge: how to connect the blockchain pseudo to a proof of the real identity. This challenge has several impacts:

1. Management of mistaken parties: for “real contracts”, a mistaken party may be recognized as a valid condition to establish contract nullity. Different countries provide different answers to this problem: while English-speaking countries void automatically the contract, the French law needs extra studies to nullify it. Focusing on smart contract, such nullity due to mistaken party, this requires certifying precisely the parties and certifying that there are no mistaken party before registering the smart contract in the blockchain.
2. Parties approving a contract must be “capable” , i.e. have a contracting capacity. This means that the party identification must be precise enough to know whether this party has the approval capacity (being major, allowed to represent an organisation…) or not. Regarding the smart contract, this involves that the blockchain user must be related clearly to the physical identity AND to the necessary information to be accepted as a smart contract validator.

To sum-up, with is immutable storage, a smart-contract defines actions in a Code is Law approach. This means that the smart contract defines a technical regulation approach whereas traditional contracts refers to legal regulation and to law organisation (which is often described as Code of Law), integrating context and usages (and potential consequences) into regulation rules. As a consequence, smart contract “legal status” is rather limited to elementary transactions (mostly defining payment conditions). In such cases, smart contracts are created and referenced once the traditional contract has been approved, avoiding by this way the problems related to parties identification.

### 2.2.2 Token and Fiat currency regulation

Tokens (or digital tokens) used in blockchain ecosystems are digital assets that can be transferred between people. These tokens (sometimes defined as coins…) may have different “kinds of value”: usage value or investment value. Usage value means that the token is associated to a granted right such as allowing to perform a task, to use a system. Usage value allows also the token owner to participate in the system governance. Security value means that the token is associated to a financial value and can be used as payment means or as investments (securities).

Tokens can be considered either as usage token or securities depending on who owns them and how they are used. To decide whether tokens are securities or not, we can refer to the Howey test. The Howey test has been set by the Supreme Court of the US (SCOTUS) in 1946 while judging ***Securities and Exchange Commission v. W. J. Howey Co.***, 328 U.S. 293 (1946). This test is used to identify what characterize investment contracts that must complies the Securities Act. Investment contract is defined as "a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party“. This means that the investor cannot take part in the common entreprise governance.

To sum-up:

- Utility tokens can be seen as a toll allowing the owner to use the network. The owner may also take part in network decision (governance, voting…).
- Security tokens are associated to money investment in a common entreprise, expecting to get profit. They must be regulated as other securities. Securities are different from commodities as commodities refer to investment on "tangible and day to day goods".
- Payment tokens are defined by Financial Market Authorities as pure cryptocurrencies, used to pay for products or services or involved in funds transfer.

Depending on the token status, different regulations may apply (or not). For example, the Initial Coin Offer associated to the Initial Funding process leads to consider the token as a security token as the initial investors do not participate to the ecosystem governance and only "bet" that the blockchain project they finance will be successful so that their tokens' value will be increased. A key point of attention is related to the way investors participate in the governance process. A simple approval voting decision is not enough as the decision is prepared and pre-validated by boards of directors / systems founders. Such a "security qualification" was decided by the SEC (Securities and Exchange Commission) in 2017 when the DAO sold billions of tokens for Ethereum, allowing investors vote for pre-selected (by the DAO board and founders) projects they want to finance and get profit from them

Figure 1 presents key criteria to qualify a token. Utility tokens mean that they grant a right such as product usage, system governance…. and / or can be associated to a function. As investments, securities are mostly associated to the expected profit. Securities can be bought or provided as "rewards" for a given work. Lastly payment tokens are associated to tolls, i.e. usage fees or simple security deposit (without expecting profits, just "to pay" with this representative commodity).

This token status guide shows that despite their initial "technical value", tokens are considered as crypto-assets so that traditional financial asset regulation should be applied.

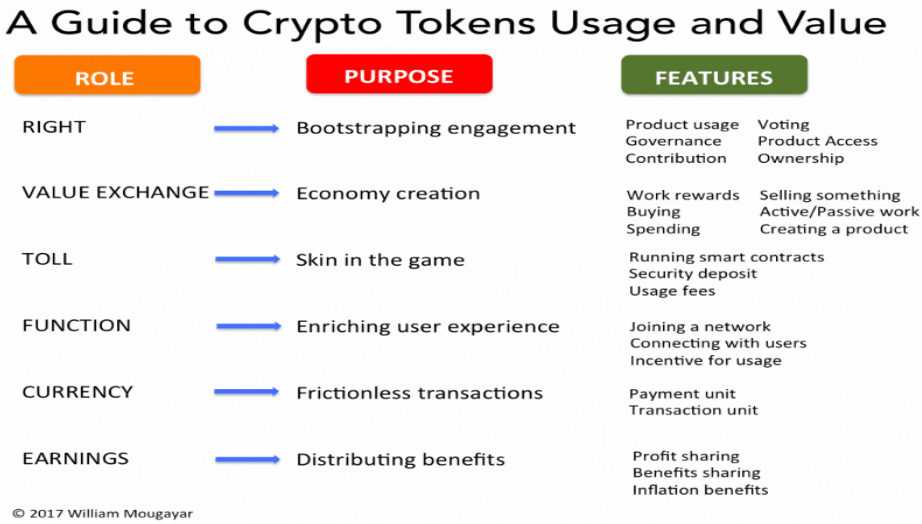



**Figure 1.** *Token classification from https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416*

This leads to identify common regulation principles for crypto assets, paying attention to the context they are used.

Initial coins offering is often used by blockchain project holders for fund-rising instead of setting a Security Token Offer (STO). To avoid the strict securities regulation, ICO are organised as utility tokens pre-sales. This means that "investors" do not invest to speculate but to get the necessary usage token (i.e. the crypto commodity) to allow their potential further usage of the blockchain service. STO are regulated as other stocks or bonds offers in order to limit risks for the investors. Depending on the ICO characteristics (quantity of issued tokens, granted usage rights, involvement in the governance organisation…) financial market authorities may re-qualify the ICO as an STO requiring to follow the strict stocks/bonds approval process. To sum-up, for the blockchain project setting an ICO sounds to be more efficient than the strict registration of an STO, but it requires paying a particular attention to the exact definition of the usage token and to the (may be risky) involvement in the shared governance.

Of course, for investors, ICO are not so different from STO, except that ICO are riskier than STO and that investors may take an important part in the project governance (for real ICO). Another important point to note is that ICO may allow anonymous participation. This refer to money laundry risks and requiring particular regulations to mitigate this risk.

This is why regulators often considers / requalifies ICO as STO so that specific regulations (depending on the country) can be applied, limiting risks for investors and preventing fraud. In other words, only STO-based fund-rising is 100% legal.

Another point to consider while identifying regulation principles for virtual assets, is the way transactions are defined. Legally, a P2P transaction requires logging traces and well-identified originator and beneficiary. Of course, the immutable storage provided by the blockchain totally fulfils the transaction logging requirement, but the pseudonymous identification of peers, related to the private key they own, does not comply the exact identification of originators and beneficiaries, leading to increase money laundry risks.

## 2.3 Virtual assets regulation

So as, we have just seen, blockchain regulation mostly refers to the financial side of the induced token economy. In this last part, we will detail the crypto-assets regulation motivation, payng a particular attention to the FinTech regulation in the EU and USA.

### 2.3.1 Regulation motivation

Let's study first why virtual assets require a dedicated regulation. As stated previously, virtual crypto-assets are de-facto representative commodities. Their value is purely speculative and not related to any tangible good intrinsic value. We must note that issuing fiat currencies is a sovereign privilege: each state can decide which currency can be used as payment means for its on economy and special agreements are set to identify the transaction support currency for international business transactions.

Currency is at the core of a state economy operation. The value of the currency is guaranteed by the value of the property held (such as the value of gold held by a central bank). Controlling the economy requires controlling financial flows, managing taxes… This is why usage of crypto-currencies is forbidden in some countries such as China, Egypt…

Crypto-assets regulation is necessary to mitigate risks:

1. Highly speculative investments are very risky for investors. Investment regulation as those used for Securities Token Offer mentioned previously provide control rules on the company issuing the token to ensure that it is a real investment and that reasonable profits can be expected
2. Uncontrolled virtual assets such as crypto-currencies may have a real impact on the "real economy": speculative and highly volatile currencies are totally disconnected from the "real good" value and costs. Using such virtual currencies and crypto-asset may lead to important financial losses depending on the way the token value varies. As these currencies are not regulated, there's no way to control their evolution.
3. Financial flows associated to virtual crypto-assets are not designed to support full "fund transfer travel data", i.e. the pseudo-anonymity of the crypto-asset owner allows using them as a money laundry system, financing criminal and terrorist systems.

This is why the Financial Action Task Force which gathered international members to regulate financial activities has proposed a world-wide recommendation to improve the fund transfer regulation and anti money laundry regulation.

The development of new crypto-assets requires widening the regulatory perimeter according to different challenges:

1. To identify clearly these new assets often used as securities and the way they are managed: traditional regulation rules must be adapt to define the ownership on a digital intangible object as several copies can be made, to allow proving the virtual object creation, defining who has the right to create and sell such crypto-assets…

2. To manage regulation territoriality constraints: as crypto-assets can be created and exchanged worldwide regulation territorial/ extra-territorial applicability conditions must be defined. Key questions refer to the identification of the "competent" territory : the traditional users country / infrastructure hosting country / provider hosting country is more complex due to the world-wide dimension of the Internet supporting these crypto-assets enactment. Moreover, defining who should regulate a virtual world (e.g.the metaverse) requires international agreements to define either "universally accepted" regulatory principles or a "metaverse" regulation authority,

3. To manage "users" / investors risks: regulation rules must be set to ensure the consumer information to warn investors about risks and controlling the "new" retail system by limiting the amounts that can be invested or checking the retailors solvency so that risks can be reduced for investors.

4. To mitigate the money laundry risk and attacks on the "real economy" due to the pseudonymous identity: this involves that crypto-assets must also comply the traditional Transfer of Fund regulation.

Focusing on the distributed ledger technology, regulation is needed:

1. To protect data stored in the ledger, referring to GDPR for personal data, to industrial secrecy regulation…)
2. To control to way such sensitive firms manage risks, setting resilience constraints to recover in case of attacks for example or requiring specific governance organisation to identify clear responsibilities and show the awareness of the governance board on risks. A particular attention must be paid on concentration of / competition between actors to be sure that the distributed organisation will remain available and viable.

Focusing on new payment systems, regulation is needed

1. To define the new regulatory perimeter in order to identify which crypto-asset can be used to support payments
2. To provide the necessary information regarding the crypto-currency and payment system (cost of a transaction, warning on the currency speculative risks or the way the payment system is governed…)
3. To control the way payment systems are governed, manage risks and organise recovery processes to guaranty the payment system availability

### 2.3.2 FATF based regulation

Let's focus on the EU Market in Crypto-Asset regulation designed to face the important financial risk associated to crypto-assets users or to new payment systems using such crypto-currencies. As these crypto-currencies are not representative currencies (i.e. they are not government backed currencies and their value is not associated to goods tangible value), they have a purely speculative value. These cryptocurrencies therefore pose a high risk to users as their prices can be very volatile. Regarding states, these non-governmental currencies can be seen as potential threatening vectors for the real economy as their unregulated prices variation can impact negatively real economy stakeholders.

These are the main reason explaining why regulating Market in Crypto-Assets is important. This leads the Committee on Economic and Monetary Affairs of the EU parliament (ECON) to adopt the MiCA regulation on October 10$^{th}$ 2022. This crypto-asset market regulation is limited to crypto-currencies (so NFT are not concerned) whatever the crypto-currency is. It constraints crypto-assets issuers (mostly the most important ones, with ore than 10 Millions users world-wide) to get an authorisation to operate in the EU. This regulation constraints crypto-asset issuers:

1. to manage "StableCoins", i.e. their token is a crypto-currency backed on a "stable and real currency" to avoid highly speculative tokens. This involves that the crypto-asset issuers must keep a liquid reserve and that these token can be claimed at anytime free of charge
2. to protect consumer wallets. They are responsible of them and must be liable if they lose investors' crypto-assets

To sum-up, this MiCA regulation aims at aligning crypto-currencies market and the traditional banking market, providing the same level of protection for investors AND the same control constraints for the token issuers.

Of course, the MiCA authorization is also conditioned by the compliance with other EU regulations such as the GDPR, the environmental footprint constraints…

Let's focus now on another major regulation challenge: the anti money laundry regulation requirement, avoiding illegally obtained money to legal money. The international diffusion of crypto-assets, the lack of precise identity control due to the pseud-anonymity makes these independent currencies convenient vectors of money laundry: by this way, tracking illegal activities through the "legal currency" exchanges, becomes harder and harder due to the pseudonymous identity used by crypto-assets systems. To improve the money laundry performances, the figure below presents an example picked from the FATF shows that there are multiple crypto-assets transactions before converting the crypto-asset into a regulated currency, making harder to identify the real source of the converted crypto-asset.

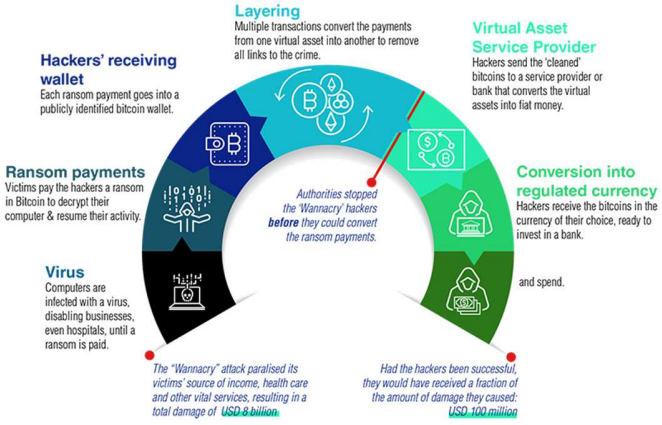



**Figure 2.** *Example of money laundry cycle picked from https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)*

Such money laundry organisation improves the profitability of illegal activities and have a great negative impact on the real economy. In the example, ransomware can lock entreprises' information systems and may lead to bankruptcy, impacting employment and the real economy. Other illegal money converting also penalize the real economy as taxes are not paid.

To sum-up, setting efficient anti money laundry regulation involves setting a universal control on the transfer of fund, providing verified travel information with the fund transfer so that money exchange can be tracked whatever the currencies and transfer of fund systems are. This involves modifying the transfer of fund regulation perimeter to integrate crypto asset systems.

Fighting against illegal activities and improving the anti-money laundry processes requires adapting the world-wide Transfer of Fund regulation requirements. As shown in the previous example, money laundry systems take advantage of the world-wide deployment of these systems and of the pseudo anonymity of crypto-asset transfer. Crypto-assets are not issued and managed by states but by technological ecosystems. Regulating crypto-assets ecosystems to reduce money laundering operations is nevertheless possible by controlling the interfaces of these ecosystems with the real economy, that is

by imposing controls on VASP. This is why mitigating this risk leads to set two main regulation requirements:

1. Fund transfer must be associated to clear and proven identities. This involves defining for each fund transfer, without any exception even for small amounts ("zero threshold" regulation), the issuer and the beneficiary and provide an end-to-end trackability. This means that
    a. Transfer operators must manage and log transfers only between issuer and beneficiary with proven identity
    b. Un-hosted wallets, i.e. wallets not held in custody by a well-identified third party cannot be accepted as issuers or beneficiaries
2. Transfer of Fund Regulation must be set world-wide allowing an end-to-end control of the financial flows. This refers to the management of territoriality constraints, leading to
    a. Identify and control virtual assets providers
    b. Manage "chained" transactions, i.e. being able to integrate intermediary VASP achieving the transfer on behalf of another
    c. Ensure that compliance measures are associated for any interaction involving a VASP from a territory where the transfer of fund regulation is set.

Similar to the traditional banking ecosystem regulation, the Financial Action Task Force, gathering international board members, proposes to set FinTech ecosystem regulation rules, extending the perimeter of traditional bank and securities market authorities' perimeters. By this way, compliant and non-compliant VASP can be registered, improving the money laundry detection processes.

These core Transfer of Fund Regulation requirements involves also paying attention to the way personal data, associated to transfer issuers and beneficiaries, are collected, stored, processed and protected. Consequently, the ToFR international recommendation from the FATF must be extended by each country to integrate its own personal data protection regulation. For example, in EU, this involves that the European Data Protection Board must be involved to define precisely rules ensuring that the regulation system will, fit the GDPR constraints.

Fighting against money laundry systems has lead EU to the development of the Transfer of Fund Regulation (ToFR). This part of the regulation aims at providing the same payment trackability constraints as those used for legal representative currencies. To sum-up it means that each fund transfer, even supported by a crypto-asset should be associated to a real identity whatever its value is (this refer to the so-called zero-threshold traceability). This involves that the associated the fund "travel information" (clear identification of the transaction issuer and beneficiary) must be stored WITH the crypto-asset transaction on both side. This means that

1: the Crypto-assets service providers (called Virtual Asset Service Providers in the EU regulations) MUST collect issuer and beneficiary identification information.

2: each VASP must log the transaction to fit the double-spending proof requirements

As crypto-currencies are not backed to any representative currencies and can be used world-wide, a main challenge is to manage territoriality / extra-territoriality constraints, i.e. how this regulation will be deployed, impacting world-wide Virtual Asset Service Providers. In fact this regulation cannot impact directly token issuers BUT it necessarily impacts the crypto-asset ecosystem by constraining VASP

operating in the EU. Existing Anti-money laundry directive obliges all companies providing crypto-related services in any EU member state, i.e. companies providing crypto-asset brokering and trading facilities.

Focusing on money laundry "facilities", un-hosted wallets (i.e. wallets not held in a custody by an identified third party) are impacted by this rule because VASP are responsible of collecting and storing information about the identity of the customers involved in a fund transfer. This involves that intermediary VASP, operating a transfer for another VASP must also be compliant regarding this fund transfer trackability, leading to make non-EU entities comply with this regulation.

Of course, tracking fund transfers and storing fund transfer "travel information" involves processing and storing personal information. This means that these information are subject to the EU GDPR. To this end, the European Data Protection Board is in charge of setting a technical specification to ensure that the transmission of these travel information complies GDPR requirements.

By integrating an end-to-end trackability to crypto-assets transfer, this ToFR regulation aims at stopping illegal flows in Europe, increasing virtual asset providers responsibility in the Anti Money Laundry process.

Let's now consider the way USA regulates the crypto-assets ecosystems. As in EU, crypto-assets were first under the "free market regulation", i.e. useful and "fair" technologies will be used and supported so that they can be developed. Nevertheless, as in EU, USA considers the financial and economic risks leading to integrate the FATF standards by extending the Bank secrecy act to integrate Digital Asset in the scope of this regulation. The key differences with the EU are the integration of NFT as "investments based on NFT" in the metaverse can take a part in money laundry systems and the reduced personal information protection, as there's no specific personal data protection in USA.

By developing digital assets regulation, USA aims at facing potential financial stability harm and increasing national security, avoiding money laundry systems related to terrorism and other criminal activities.

Similar to EU, the US regulation fits the FATF challenges to support a responsible development for virtual assets, avoiding the "jungle-law based" development of highly speculative systems. This leads to regulate fund transfer by integrating "travel information" in the transfer transaction and regulate digital securities in a similar way as traditional securities, enforcing the link between virtual assets and real world representative currencies and protecting investors and virtual asset deposit.

## 2.4 Conclusion

So, after introducing the regulation context, defining blockchain regulation key principles and paying a particular attention to virtual assets regulation, it's now time to conclude.

Blockchain regulation aims at defining a legal status of this technology and regulate its related usages. In this lecture, we introduced the regulation context, identify the legal definition of blockchain and addressed the legal status of token and smart contract. In this presentation, we can see that these legal status and key regulation principles are similar to those regulating contracts and securities.

As the blockchain technology is used as a major driver for FinTech development, we paid a particular attention to the virtual asset regulation. Even if regulation is set by each country, we have seen that common regulation principles have been set by the FATF, leading to similar regulations. By controlling the way digital assets ecosystems interact with the real economic world, fund transfer and market in crypto-assets regulations are set to support responsible digital assets development.

Further regulation constraints related to GDPR and personal data protection in blockchain environment will be discussed in lecture 6.

# 3 PRACTICAL EXERCISES

This practical exercise shows how you can identify some blockchain regulation and governance challenges. The case study used in the different exercises from this module is based on a supply-chain / industry 4.0 case study.

Let's consider the organisation of a "producer to consumer food supply-chain". Different producers are involved in the food procurement and transformation. Each member of the supply-chain ecosystem can integrate its own suppliers in a "sub-supply chain". In order to eliminate wastes, the supply chain is managed in a Just in Time strategy. Increasing the product quality and the production transparency leads to track each product / transformation process so that consumers can be called in case of trouble.

Identify which regulation principles may be applied to this use-case.

To solve this problem, you need to identify

- The ecosystem organisation and the way the system is created
- If smart-contracts are created and their purpose
- The kind of information stored in the blockchain

For each topic you need to ask some Who / What / For What / From where / Why / How questions

- The business-oriented ecosystem relies on the collaborative networked production organisation. As seen in lecture 3, this is a partner-centred organisation. Focusing on the blockchain system enactment, identify the token status, the way ecosystem members can get and use these tokens
- Focusing on the blockchain organisation, identify what is stored in the blockchain and the associated regulation constraints
- Identify different kinds of incentives to support such a system

Analysing the requirements shows that:

- The business-oriented ecosystem relies on the collaborative networked production organisation. As seen in lecture 3, this is a partner-centred organisation. Focusing on the blockchain organisation, we can identify different strategies depending on the project genesis:
    a. The main stakeholder may be the unique owner: this happens if the main stakeholder provides the full blockchain infrastructure and constraints its partner to register their production in the blockchain. This means that the project owner will support the full cost of the blockchain and will sell the blockchain service to other parties
    b. The project may be launched as a common answer of all participants to regulation constraints / quality processes / main clients requirements… In such case, all partners

involved in the supply chain are founding members. Paying attention to their initial investment, they can get utility tokens based on their initial investment and take parts in the system governance. This means that the initial fund rising can be considered as an ICO

- Focusing on the blockchain organisation, we can identify that a permissioned blockchain may be set. Such “private” blockchain deployment limits the speculation risks associated public blockchain backed systems.
- Focusing on the information stored in the blockchain: it should contain only production data, protected by the industrial secrecy. Information sourcing is required to ensure the full trackability of products.
- Such system design must be compliant with food industry regulation

# 4 CASE STUDIES

## Agri-food NFT Case study

A group of agri-food entreprises want to set a NFT based loyalty program associated to the product they sell. Each company will provide some “loyalty score” depending on the customer activity. These loyalty scores are managed by a dedicated entity. Each customer can apply for a given NFT attached to a rare “real product” provided that he gets enough validated loyalty score. These NFT are used to grant access to the product ordering. Identify the key characteristics of the associated blockchain project, discuss the deployment to decide which regulation rules can apply..

or

Choose an example of blockchain project and analyse it in a similar way as what was done in the exercise.

# 5 QUESTIONS AND ANSWERS

## Description

## Question and Answer No.1

**Q:** What does blockchain regulation mean?

**A:** Blockchain regulation defines the set of legal rules controlling the interaction of blockchain ecosystem with its environment.

## Question and Answer No.2

**Q:** Is there a unique world-wide regulation for blockchain?

**A:** As other regulation rules, blockchain regulation integrates territoriality constraints. As a consequence, there's not a unique world-wide regulation for blockchain.

## Question and Answer No.3

**Q:** What is the legal status of smart contract, is it similar to traditional contracts?

**A:** Smart contract defines P2P transactions. It is different from classical contracts as parties may be defined thanks to avatars. They are considered as an implementation of simple rules defined in classical contracts.

## Question and Answer No.4

**Q:** What is the legal status of blockchain tokens?

**A:** Blockchain tokens may have different status depending on their usage. There may be payment tokens, utility tokens or security token

## Question and Answer No.5

**Q:** What is the meaning of AML?

**A:** AML means Anti Money Laundry

# 6 MULTIPLE-CHOICE QUESTIONS

## Multiple Choice question No. 1

**Q:** Blockchain regulation defines rules controlling

**A**: The interaction of the blockchain ecosystem with its environment

- The interactions between blockchain ecosystem participants
- The interaction of the blockchain ecosystem with its environment
- The self-adaptation of the core blockchain algorithms to optimize it depending on the context

## Multiple Choice question No. 2

**Q:** Blockchain 1.0 challenges regulation regarding

**A**: Fiat currencies and securities

- Fiat currencies and securities
- Smart contract status
- Transaction tracking

## Multiple Choice question No. 3

**Q:** The first time Blockchain legal status has been defined was in

**A**: 2015

- 2009
- 2015
- 2018

## Multiple Choice question No. 4

**Q:** Smart contract legal status

**A**: is defined as an implementation of a legal P2P contract

- Is similar to a classical contract
- is defined as an implementation of a legal P2P contract
- is not defined

## Multiple Choice question No. 5

**Q:** When an investor cannot participate to a blockchain governance, the token must be considered as

**A**: A security token

- A payment token
- A utility token
- A security token

## Multiple Choice question No. 6

**Q:** Which fund rising strategy is the most protective for the investors

**A**: STO

- STO
- ICO

## Multiple Choice question No. 7

**Q:** The Transfer of Fund Regulation aims at

**A**: tracking chained transactions to avoid money laundry

- Increasing the fund transfer efficiency
- Reducing the cost of fund transfers
- tracking chained transactions to avoid money laundry

## Multiple Choice question No. 8

**Q:** Crypto-assets are

**A**: purely speculative currencies

- representative currencies
- purely speculative currencies
- basic securities

## Multiple Choice question No. 9

**Q:** The EU MiCA aims at setting

**A**: Stablecoins, i.e. integrate liquid reserve and avoid speculation on tokens

- Interoperable crypto-assets
- A free market to support blockchain end crypto-currencies development

- Stablecoins, i.e. integrate liquid reserve and avoid speculation on tokens

## Multiple Choice question No. 10

**Q:** EU and USA transfer of fund regulation

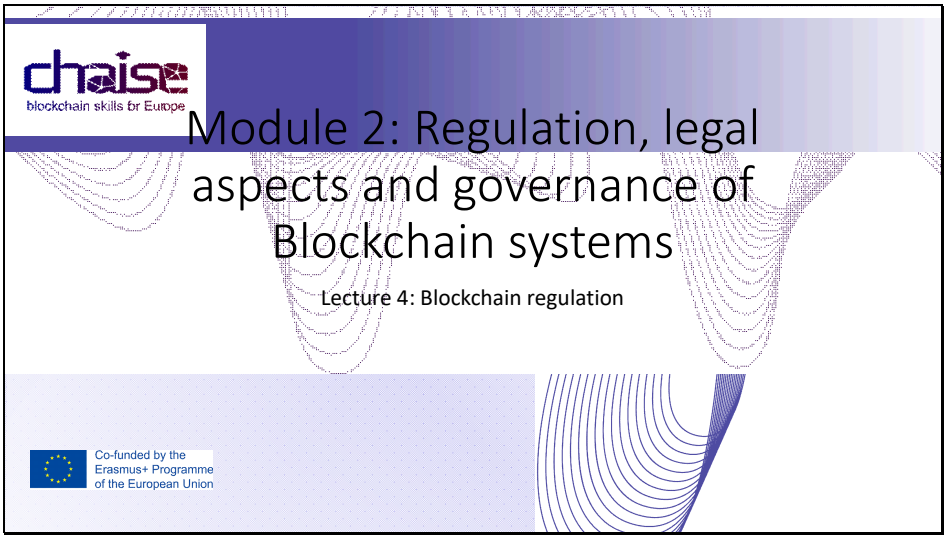
**A**: do not cover the same perimeter as USA includes NFT

- Are totally similar
- do not cover the same perimeter as USA includes NFT and EU is restricted to crypto-currencies
- do not cover the same perimeter as EU includes NFT and USA is restricted to crypto-currencies

# 7 REFERENCES


- Library of Congress. Regulation of Cryptocurrency around the world. 2021. https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf
- https://www.legal500.com/guides/guide/blockchain/
- Blemus, Stéphane, Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide (January 17, 2018). Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF N°4-2017 - December 2017, Available at SSRN: https://ssrn.com/abstract=3080639 or http://dx.doi.org/10.2139/ssrn.3080639
- Hughes, S. D. (2017). Cryptocurrency Regulations and Enforcement in the US. *W. St. UL Rev.*, *45*, 1.
- EU MiCA proposal: https://data.consilium.europa.eu/doc/document/ST-11053-2020-INIT/en/pdf
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/
- KPMG. Regulation and supervision of Fintech. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf
- https://www.fatf-gafi.org/


# 8 Slides



| 2. REGULATION, LEGAL ASPECTS, AND GOVERNANCE OF BLOCKCHAIN SYSTEMS | | |
|---|---|---|
| Explain blockchain-related regulations, legal aspects, governance, and their impact in the public and private sectors. | | |
| Knowledge | Skills | Responsibility and Autonomy |
| Knows / Aware of:<br>- Blockchain-related legal environment.<br>- Legal underpins of Blockchain technology and smart contracts.<br>- Legal implications of cryptocurrencies.<br>- Blockchain and public policy, governmental regulations | Able to:<br>- LO2.1: Describe blockchain-related legal environment in Europe and the World.<br>- LO2.2: Explain regulatory framework of blockchain based financial services.<br>- LO2.3: Recognize legal and regulatory issues and risks when dealing with cryptocurrency and blockchain technology. | Capable to:<br>- Practice critical thinking of the blockchain legal environment and regulations.<br>- Take responsibility when deciding about the blockchain, cryptocurrencies and use of smart contracts. |
| EQF level | EQF Level 5 | |

# Blockchain regulation?

- What are the motivations regarding regulation?
- Is regulation “location dependent” or not?
- Is there a specific regulation for Blockchain or should other regulations apply?
- Are there some usage dependent regulation?

## Understanding blockchain regulation challenges?

- In this lecture you will
  - Learn key regulation principles
  - Identify blockchain key regulation requirements
  - Learn virtual asset protection context
  - Learn applicable regulation mechanisms applied to blockchain usages

## Learning objectives

| Regulation context | Blockchain key regulation principles | Virtual assets regulation |
|---|---|---|
| Technology vs usage regulation | Incentives and key technic regulation | Motivation and key risks |
| Key blockchain regulation challenges | Token and Fiat currencies | FATF-based regulations |

# Table of Content



chaise
blockchain skills for Europe

Co-funded by the
Erasmus+ Programme
of the European Union

# Regulation : context

- Definition
  - An official rule or act
    - Government / authority
    - Specific validation processes
  - Checking whether a business follows or not official rules / laws
  - Social rules
- Regulation
  - Different contexts
  - Primary / secondary laws
  - Territoriality / extraterritoriality

## Business regulation

- Contracts are necessary
  - To identify parties
  - To identify the purpose
  - To have a common legal reference
- Contracts can be stored in a blockchain
  - Automatized signature protocol
  - Pay attention to trades secrecy
- Blockchain-based business development
  - Public blockchain for short term : reduced investments
  - Consortium / private blockchain for long term collaboration
  - Keep in mind that different legal framework may apply

8

## Techology vs usage regulation

- Technology
  - “Inert object”
  - Implementation
  - Usage
- Technology regulation
  - Core development regulation
  - Usage regulation
    - Social impact
    - Economic impact
    - Environmental impact
    - …
  - Territoriality?

## Key technologic requirements

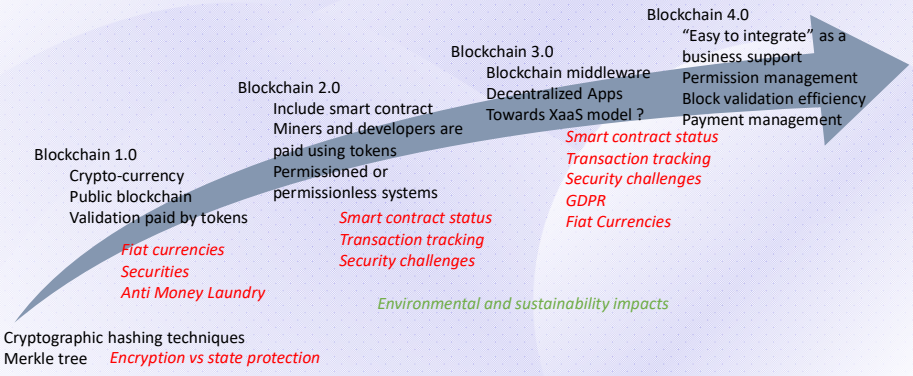
- P2P transaction support
  - Solve and prove the double-spending problem
    - Previous interchange contracts manages logs on each system
    - Blockchain integrate the double spending process as its core service
  - Immutability management and trackable processes must be deployed
- Cryptography
  - Used to “sign transactions”
  - Has different regulations depending on the countries
  - Limits regarding authentication
- Distributed architecture
  - Identifying / proving responsibilities limits
  - Token exchanges are trackable but not the way blocks are validated (means involved)
  - Threats can focus on different entry points



## Key socio-economic requirements

- Environmental impact
  - Authorizations to set data centers
  - Require estimating the energy consumption
- Token economy
  - Token status:
    - Transnational and unregulated crypto-currencies
    - Technical value
  - Different legal constraints depending on the countries
- Complexity of blockchain governance
  - Different blockchains used for different purpose
  - No transfer between blockchains
  - Governance rules compliance

## Blockchain regulation challenges




## Table of Content

- Regulation context
  - ❑ Technology regulation
  - ❑ Blockchain regulation challenges
- Blockchain key regulation principles
  - ❑ Incentives and key technic regulation
  - ❑ Token and Fiat currencies
- Virtual assets regulation
  - ❑ Motivation and key risks
  - ❑ FATF-based regulations (MiCA, ToFR)
- To conclude

## Blockchain incentives

- Economic incentives
  - Data center hosting
    - Activity development
    - Taxes on energy can be used to regulate these deployments
  - Target “sovereign blockchains”
    - Based on the computing/storage infrastructure
    - Be sure that only one legal context is applicable
    - Does not fit the public blockchain openness target
- “Regulation” incentives
  - Sandboxes
  - Technology development and evaluation

14

## Blockchain legal status

- 2015 – France law “Macron 2”
  - French government can authorize distributed ledgers for issuance and recording mini bonds
  - Associated transactions can be recognized as legal contracts
  - Extended to registered financial instruments
  - Establishment of a legal framework
- USA: March 2017
  - Arizona House
  - a “distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is theoretically immutable and auditable and provides an uncensored truth”

## Smart contract

- Automated transaction vs legal contract?
  - Implementation of a “real world contract”
  - Limited process
- Contracting involves
  - Identified parties
    - How to connect “True identity” with Blockchain pseudo?
    - Mistaken party may involve (or not) contract nullity
  - Contracting capacity
    - How can you prove that the pseudo-identified party is allowed to contract?
    - For example only major people can sign a contract. What about minors?
- Code is law vs Code of law
  - From technical to legal regulation
  - Usage and context

16

## Token and crypto assets

- Token status
  - Usage value
    - Necessary to perform a task / use the system
    - Transaction fee is a toll
  - Security value
    - Payment mean
    - Money investment
- Howey test (US) to identify securities
  - Money investment in a “common” entreprise
  - Expected profit
  - No possibility to change the entreprise governance

17

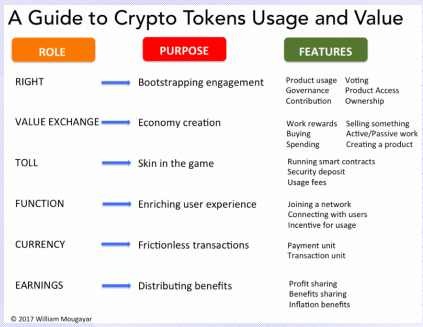
## Token value

- Depend on the actor and on the project
  - Utility token
    - Allow using the network
    - Involved in the governance
  - Security token
    - Money investment
    - Bet on a project to get profit
  - Payment token
    - Pure crypto-currencies
    - Pay for products or fund transfer
- Different regulation rules apply for the Initial Funding process



## How to qualify a token?

- Utility
  - Right
  - Function
- Security
  - Earnings
  - Value exchange?
- Payment
  - Toll
  - Currency
  - Value exchange?




Source: https://medium.com/@wmougayar/tokenomics-a-business-guide-to-token-usage-utility-and-value-b19242053416

# Key regulation principles for Virtual assets

- Initial coin offering
  - For the blockchain project
    - Fund rising
    - Less regulated than the financial market?
  - For investors
    - Securities investment
    - Be integrated in the project governance
  - For regulators
    - Securities
    - Specific regulation authorities depending on the countries
    - Fraud prevention
- Transactions
  - Traces
  - Originator and beneficiary identification


Source: https://fr.cryptonews.com/guides/the-difference-between-ico-and-sto.htm

# Table of Content



chaise
blockchain skills for Europe

Co-funded by the
Erasmus+ Programme
of the European Union

## Regulation motivation

- Sovereignty
  - Fiat currency management
    - Crypto-assets may be forbidden (China, Egypt…)
  - Taxes
- Risks
  - Investors
  - "Real" economy impact
  - Criminal and terrorist financing systems
- World-wide recommendation
  - Financial Action Task Force (FATF)
  - Anti Money Laundry

## Fintech related emerging regulation requirements

| | Crypto-asset | Distributed ledger technology | Payment systems |
|---|---|---|---|
| Changing regulatory perimeter | X | | X |
| Disclosures to consumers | X | | X |
| Limits on retail investors access | X | | |
| Governance of firms | | | X |
| Firms' risks management | | X | X |
| Operational resilience of firms | | X | X |
| Data protection | | X | X |
| Anti money laundry | X | | |
| Concentration and competition | | X | X |

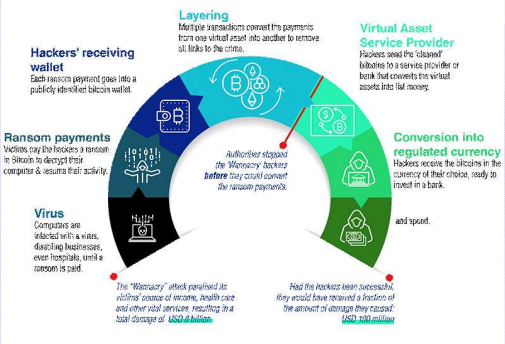
Source: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf

## EU Market in Crypto-Assets

- Designed to face crypto-assets risks
  - Consumer protection
  - Monetary sovereignty
  - Exclude NFT
- Crypto-Asset service providers
  - Authorisation to operate in EU
  - Consumer wallets protection
  - Liable if they lose investors' crypto assets
- Environmental footprint declaration
- StableCoin
  - No speculation
  - Liquid reserve
  - Free of charge claim at any time

## Anti Money Laundry requirement

- Money laundry life-cycle
  - International coins
  - Lack of identity management
  - Independent currencies
  - Multiple actors
- Real impact on economy




Source: https://www.fatf-gafi.org/publications/virtualassets/documents/virtual-assets.html?hf=10&b=0&s=desc(fatf_releasedate)

# Key ToFR regulation requirements

- Real identity
  - Proven identity
  - No transfer Threshold
  - Issuer and beneficiary identities collected and stored by Virtual Asset Service Provider in charge of executing a transfer
  - Impacts also unhosted wallets (i.e., wallets not held in custody by a third party)
- International scope
  - Companies providing Virtual Asset Services in EU
  - Enhanced compliance measures for any interaction between EU and non EU VASP
  - Include intermediary VASP i.e. achieving a transfer on behalf of another one: transmit initial originator and beneficiary along the chain
- Regulation operation
  - European Securities and Market Authority (ESMA)
  - European Bank Authority (EBA)
    - Non compliant VASP register
- Data protection
  - European data protection law: GDPR
  - Application conditions defined by the European Data Protection Board

# EU Transfer of Fund Regulation

- Virtual asset
  - Similar to traditional financial services
  - Pseudonymous transactions
- Financial “travel rules”
  - Proven identities
  - Source and beneficiary information associated to the transaction
  - Safe storage of the transaction on both side
- Stop illicit flows in EU
  - Transfer the “travel rules” to crypto assets
  - Crypto asset service provider responsibility
    - Store the transaction
    - Check if the source is reliable

# USA key regulation

- Evolving regulation
  - Digital assets including NFT
  - From free market regulation to Bank secrecy act integration
  - Face financial stability harm and national security
- Similar FATF challenges
  - Responsible development of Virtual Asset
  - Fund transfer control
  - Securities regulation

# Table of Content



chaise
blockchain skills for Europe

Co-funded by the
Erasmus+ Programme
of the European Union

# To conclude

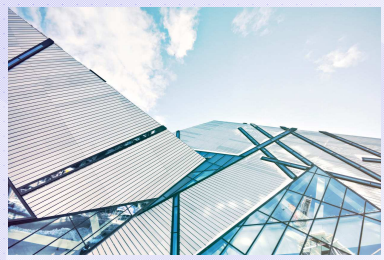
- Regulation
  - Legal control
  - Technology vs usage
- Blockchain regulation challenges
  - Legal definition
  - Smart contract status
  - Token
- Virtual asset regulation
  - Financial stability
  - Customer protection
  - Transfer of Fund regulation

chaise
blockchain skills for Europe

Co-funded by the
Erasmus+ Programme
of the European Union

# Resources


- Library of Congress. Regulation of Cryptocurrency around the world. 2021. https://tile.loc.gov/storage-services/service/ll/llglrd/2021687419/2021687419.pdf
- https://www.legal500.com/guides/guide/blockchain/
- Blemus, Stéphane, Law and Blockchain: A Legal Perspective on Current Regulatory Trends Worldwide (January 17, 2018). Revue Trimestrielle de Droit Financier (Corporate Finance and Capital Markets Law Review) RTDF N°4-2017 - December 2017, Available at SSRN: https://ssrn.com/abstract=3080639 or http://dx.doi.org/10.2139/ssrn.3080639
- Hughes, S. D. (2017). Cryptocurrency Regulations and Enforcement in the US. *W. St. UL Rev.*, *45*, 1.
- EU MiCA proposal: https://data.consilium.europa.eu/doc/document/ST-11053-2020-INIT/en/pdf
- https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/
- KPMG. Regulation and supervision of Fintech. https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/03/regulation-and-supervision-of-fintech.pdf
- https://www.fatf-gafi.org/

chaise
blockchain skills for Europe

Co-funded by the
Erasmus+ Programme
of the European Union

chaise
blockchain skills for Europe

# Get In Touch

**Social Media**

@ CHAISE.EU

**Website**

chaise-blockchainskills.eu

**Email**