HAL
open science

ERASMUS + Chaise Project - Module 2: Regulation, Legal aspects and Governance of Blockchain systems Lecture 1: Blockchain basics to set the regulation and governance context and requirements

Frédérique Biennier

To cite this version:

Frédérique Biennier. ERASMUS + Chaise Project - Module 2: Regulation, Legal aspects and Governance of Blockchain systems Lecture 1: Blockchain basics to set the regulation and governance context and requirements. INSA Lyon. 2022. hal-03852378

HAL Id: hal-03852378

https://hal.science/hal-03852378

Submitted on 15 Nov 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

blockchain skills for Europe

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

Lecture 1: Blockchain basics to set the regulation and governance context and requirements

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 3

2 LECTURE NOTES 4

2.1 BLOCKCHAIN KEY CONCEPTS 4

2.1.1 Key concepts 4

2.1.2 Provided service 5

2.1.3 Blockchain typology 5

2.1.3.1 Access control criteria 5

2.1.3.2 Blockchain technology criteria 6

2.1.4 Key governance and regulation challenges 7

2.2 BLOCKCHAIN AS A DISTRIBUTED ORGANISATION 7

2.2.1 Core governance rules 7

2.2.2 Usage context 9

2.2.3 Token related requirements 9

2.3 KEY GOVERNANCE AND REGULATION REQUIREMENTS 10

2.4 CONCLUSION 11

3 PRACTICAL EXERCISES 13

4 CASE STUDIES 15

5 QUESTIONS AND ANSWERS 16

6 MULTIPLE-CHOICE QUESTIONS 17

7 REFERENCES 20

8 SLIDES 21

1 INTRODUCTORY PARAGRAPH

In this second module, we focus on the way blockchains are governed and regulated. In this first lecture, we identify the key characteristics of the blockchain systems to identify the potential usages and the blockchain ecosystem characteristics to identify key governance rules used to managed interactions in the blockchain ecosystem and regulation requirements to regulate interactions of the blockchain ecosystem with its environment.

How can we identify such requirements? What do you think regarding this challenge?

According to you, is there a unique generic blockchain system model that can be used to capture governance and regulation requirements?

As governance rules are set to manage internal interactions of actors involved in the ecosystem, can we define some key characteristics from which governance requirements can be derived?

Defining the way the blockchain system interacts with its environment involves paying attention to its actors, their motivation and the interaction they have with their environment to identify which regulation context must be applied

Lastly, should the different blockchain usages involve a regulation?

To answer these questions, we will first characterize the blockchain systems to identify the way internal governance rules are set. Then we will pay attention to the blockchain ecosystem organisation, to the different application fields to capture regulation requirements

To sum up, this lecture addresses different learning objectives regarding

1. Blockchain key characteristics, introducing a blockchain typology
2. Blockchain as a distributed interaction to identify which internal governance rules are necessary and paying a particular attention to the token status
3. Regulation and governance requirements, paying a particular attention to the blockchain ecosystem and the way it interacts with its environment

2 LECTURE NOTES

2.1 Blockchain key concepts

2.1.1 Key concepts

Basically, a Blockchain is a digital and distributed transaction ledger. Transactions are stored in blocks and blocks are chained. We can note that this mechanism is independent of the content associated to the transaction which can be associated to a payment, to an automated process, a granted access, a certified information…

As a distributed system, there are no trusted tier in charge of authenticating the transaction. Trust relies on the way the distributed ledger is built and ensure a safe and immutable storage of the transactions as well as transaction non-repudiation. These 2 characteristics must be considered while setting governance and regulation.

How can these requirements be implemented in a distributed organisation?

First works achieved in 1991 by Stuart Haber et W. Scott Stornetta from Bell Labs have introduced cryptographic hashing techniques to set a « document digital signature », including both the document and the time stamps which allows storing immutable records. The distributed ledger is organized thanks to Merkle Trees which were introduced in 1979 to store the « hashed » information. Each leaf stored a hashed document. Then blocks are merged and a new hash based on these two signatures is computed and inserted in the tree higher level, and so on. Merkle trees are binary trees so extra empty nodes can be added to ensure a binary tree is always produced. This binary tree organization allows achieving local checks on a sub-tree so it can be checked even if nobody has the full tree structure. Local control on a block involves getting hash from its « brother » so the father hash can be computed. Then this father hash is combined with its uncle hash value and the next layer can be checked. These former works provide the cryptographic background to support blockchain. A block contains both transaction data and a hash of the previous block. Integrating cryptographic blocks can be used to prove data integrity, provided that the tree has not been attacked.

Focusing on transaction non-repudiation, such a feature is traditionally proven by logging all processing actions in different ledgers (one managed by each party involved in the transaction) so that each partner can show how the distributed process is run on its side. Organizing a distributed ledger storing the same Merkle tree on several hosts increase availability and robustness. But this leads to a new challenge: how to protect the ledger from changes and how to ensure trust between the different systems hosting a copy of the leger. This means that the block chain has its own governance rules, accepted by all participants so that the decision process can be decentralized and it does not require a certification authority. Different protocols govern blockchain transaction validation: proof of work, proof of stakes… Distributed means that several synchronized copies of the ledgers are available. This increases the global security level as hacking a blockchain involves hacking at the same time the different instances of the ledger.

At this point we can see that the block validation rule must be defined to govern the blockchain organisation.

2.1.2 Provided service

Blockchain provides a new service to store P2P transactions, solving the double spending problem as a single chain of blocks approved by both parties is built. In traditional transactions, party identity and transactions are certified thanks to authorities, managing a secured deposit. Authorities are well known and warranty the "true identity", sometimes thanks to the deposit of "physical proofs". Consequently, traditional transactions have a price to pay the service provided by one of these authorities.

The Blockchain is a distributed organization. Each member of the community invests (computation resources, currencies…) to validate a transaction

When a blockchain is used to store a transaction, trust is associated to the block validation protocol. This leads to set a distributed trust management protocol, relying on consensus management between the nodes hosting a copy of the ledger.

Similar to other services, registering a transaction in a blockchain has a cost and fees must paid. Consequently, instead of paying transaction fees to traditional authorities, these fees can be negotiated with transaction validators. Depending on the chosen validation fees, different transaction priorities can be set to favour a faster or slower validation process. Transaction fees are "paid" with tokens managed by the blockchain itself. This provide a state-independent currency management BUT validators need to "sell" these crypto-currencies to pay for "real world" resources they use to achieve the validation job. As a crypto-currency is set, regulation rules are necessary as money creation is a Regal privilege.

2.1.3 Blockchain typology

2.1.3.1 Access control criteria

Let's now try to characterize the blockchain system to identify a blockchain typology.

As a first criteria we can set blockchain access control to characterize the blockchain system. This leads to split blockchain systems into permissionless and permissioned blockchains.

To provide opened and publicly shared ledgers, no access control is required. As a consequence, such public blockchains are called permissionless. These permissionless blockchains are fully opened to both users and validators who only need to follow the block validation protocol and provide the requested resources to mine blocks. In such public systems, participants are identified thanks to an avatar, a kind of pseudonymous, which provide them the ability to sign for a transaction without providing their real identity to the blockchain system.

On the opposite a private blockchain system is designed for well-known participants, i.e. participants with an authenticated and authorised identity. This leads to implement access control to grant access permissions to the blockchain. Such systems are called permissioned blockchains. In such systems, validators are restricted to authorised ones, so trust management is simpler and a large variety of

consensus protocols can be used. Such permissioned blockchains can also be set for well-identified consortium, leading to consortium blockchain.

Hybrid blockchain systems are permissioned systems, protecting the transaction confidentiality BUT transactions can be verifiable.

2.1.3.2 Blockchain technology criteria

Since the introduction of the first Bitcoin blockchain system, blockchain technology has evolved, allowing us to define a 2nd blockchain system classification criteria: the blockchain technology.

Based on this technology criteria, we can identify a 4-element typology.

1. The oldest technology is called Blockchain 1.0. It provides a permissionless public blockchain system supporting crypto-currency based transactions. Blockchain developers and block validation are "paid" thanks to tokens used as fiat currencies. Nevertheless, these cryptocurrencies introduced to support P2P currency transfer without any intermediary, are disconnected from any valuable good exchange: there is no real link with any actions in the "real economy" nor any unified international market. Moreover, these crypto-currencies are isolated from each other. Their pricing, expressed in traditional currencies, are highly volatile due to speculation from core developers and miners who optimize the revenue they get from operating the blockchain and transaction validation service. Users are associated to an avatar and a cryptographic key, without having to prove their real identity. This leads to consider such cryptocurrencies as "launder currencies" for the dark economy

2. Similar to Blockchain 1.0, Blockchain 2.0 developers and transaction validators are paid thanks to token. Nevertheless, Blockchain 2.0 are not designed as crypto-assets, they introduce a new mechanism to support value-added usage development for the blockchain: the smart contract. Blockchain 2.0 technology can support both permissioned and permissionless blockchains. A smart contract is a computerized transaction protocol with a fully automatized execution. The code is stored in the blockchain as the transaction content and is executed according to activation conditions. The smart contract execution is associated to assets transfer, providing a link between a token and a "valuable" service. As in the "real" contracts, contract terms represent the valuable good/service that must be executed to support the token transfer. All nodes involved in the blockchain must execute the smart contract, allowing the token transfer. To sum-up, smart contracts provides a more reactive data-driven / event driven distributed organization than the traditional control flow organization of IT systems.

3. Blockchain 1.0 and 2.0 have provided technological supports for public usage. However, sharing blocks in a public infrastructure may be risky for enterprises. Permissioned blockchains provide private and isolated distributed support for a company or a consortium but they require first to know precisely who can accede to the blockchain and there is no solution to manage inter-blockchain exchanges. To overcome these limits, Blockchain 3.0 aims at providing blockchain middleware, providing interoperability and scalability. This leads to Blockchain as a service

organization, embedding blockchain technology (and may be extra usage-based services) into more "traditional" XaaS vision.

4. Blockchain 4.0 aims at embedding the blockchain technology into a more business-friendly organisation. Whereas blockchain 2.0 and 3.0 require development and technological knowledge, blockchain 4.0 aims at empowering users with a simpler development process. It provides extra functions based on the blockchain 3.0 stack such as access control, payment management. It also addresses the blockchain efficiency limits to support large scale deployment.

2.1.4 Key governance and regulation challenges

Based on this short review of blockchain characteristics, we can identify a set of governance and regulation challenges.

First of all, all blockchains are designed as distributed organisations, integrating different kinds of actors (developers, transaction validators, users…). This means that governance rules must be set and accepted by all parties to define the validation strategy, the way transaction validators are paid as well as access control mechanisms to join the distributed application.

Focusing on the main functionality of the blockchain, managing a distributed ledger storing immutable and trusted transactions, it can be used by applications from various areas. This lead to integrate regulation challenges related to the anonymity of the users, the token status… These points will be discussed in the further sections.

2.2 Blockchain as a distributed organisation

After identifying the core blockchain key characteristics, let 's now first identify the way such distributed organisations are governed, i.e. the way decision are taken. As tokens are often used to « pay » miners and core developers, we will also focus on the token status t identify whether which governance or legal regulation are set to regulate these tokens usages.

2.2.1 Core governance rules

As said previously, blockchain is a distributed trust system with multiple stakeholders. The initial Blockchain 1.0 has been set an opened system which can be joined freely by transaction validators. The key governance question for such an organisation is: can we ensure that the distributed ledger is safe, immutable and consistent? In fact, trust is necessary to validate the transaction and ensure that each copy of the distributed ledger stores the immutable and validated transaction. This involves that all stakeholders must accept and share a common decision rule to define how a block can be validated and inserted in the leger.

In this distributed ledger context, trust building refers to the Byzantine generals problem: the challenge consists in getting a consensus to prove the validity of the distributed ledger even if some of its copies are modified by felon agents. Such governance rules are designed to be safe provided that there are no "secret validators organisation" aiming at providing a consensus on "false block validation": in such a

case, all miners involved in the felon organisation declare that the false copy is the right one and if they are a majority, all others must accept it.

To manage the distributed ledger consistency, different consensus management strategies are used. The key point consists in determining the "right" trusted value from information stored in different ledgers. Basically, the problem has been addressed thanks to Byzantine Fault Tolerant algorithms (such as Raft or Paxos). These algorithms can identify the trusted ledger value, if 51% of the nodes are not lying. Other new approaches, such as gossip-based consensus, are introduced (Hashgraph). In this last case, each network member adds a new "comment" and send the block to the next node (may be chosen randomly). Paying attention to the protocols to validate a transaction, inserting it in a block linked to previous ones, different blockchain consensus rules can be used:

1. Proof of Work is the first protocol introduced in the blockchain 1.0. It involves complex mathematical problem solving. The key idea is that an often-important investment is required to get the transaction validation. This work involvement of the blockchain miner is associated to the trust level it can have. On one hand, it is also rather hard to generate the validation information so that the transaction integrity is increased (too expensive to be hacked) but on the other hand, important pools of computing resources and energy are required to support the blockchain. Therefore, miners, who are paid using blockchain certified crypto-currency, have to sell this crypto-currency to get "legal currencies" to buy these computing resources and energy. Consequently, this increases the speculative character of these currencies.
2. Proof of Stake avoids heavy computations. In this case, validators are randomly chosen according to the amount of currency they invest for the transaction. To avoid a "centralized" validation architecture (i.e. a system where always the main owner of the currencies can validate transactions), regulating mechanisms are set for example requiring a minimum time storage for the currencies, integration of past successful validations… This means that more a validator invests higher is the probability to validate blocks and get the money for this. As there is reduced computing costs, there is less need to speculate and have an inflationist crypto-currency system. As Proof of Stakes blockchains uses proofs of crypto-currency owning (instead of computing resources) to validate new blocks instead of "investing computing time". Therefore, in this context the 51% trusted nodes attack means that the attacker need to possess at least 51% of the crypto-currencies.
3. Proof of Authority: In such case, a small number of well identified players, who do not naturally wish to cooperate but benefit from doing so are operating as validators. Trust is built according to what validators have to lose in the event of malicious acts. This is a rather "centralized" organisation. Validators are chosen depending on their reputation. When a validator validates a block, the other must vote to accept it. This means that the validator has to "proceed with the job fairly" otherwise, it will not be approved anymore. Using such a validation strategy involves that validators are "elected" by others on a fair basis, i.e., a validator cannot validate 2 consecutive blocks for example. The main limit of this strategy is that the "validation power" is owned by a reduced set of validators. The main advantage is that Blocks are validated quickly at almost "no cost".

You can view on https://www.youtube.com/watch?v=0RmgcGFKoGM a simplified introduction to these consensus mechanisms

2.2.2 Usage context

Other governance rules can be identified based on the blockchain characteristics. As mentionned in the first part of this lecture, there are permissionless and permissioned blockchains.

For permissionless blockchain, no access control rules are required. Users can participate depending on the blockchain potential market. This mean that the initial actors must agree to set a convenient community development strategy.

Regarding permissioned blockchains, extra rules regarding access control must be defined. Basically, either participants are fixed from the initial system definition or a dedicated co-optation mechanism must be set to grant access to the private blockchain. This authorisation rule must be set initially and ought to be immutable. As the blockchain provides a transaction validation service, its operation entails costs and it is important to clearly define rules for sharing them.

Regarding hybrid blockchain, which are often community based permissioned blockchain, there are sets of rules to define public / private services from the blockchain and which user can invoke which service.

2.2.3 Token related requirements

Cryptographic tokens are the core digital assets managed by a blockchain. A token belongs to a blockchain address which provide a pseudo anonymity for the owner. Each owner has its own private cryptographic key, stored in a wallet. This key is used to sign a token before sending it to another person. By this way the token ownership is transferred. By this way, tokens can be exchanged without duplication.

Tokens can be associated to access rights, to a set of rules coded in a smart contract or to a payment mean. They can be granted to validators as a reward for the block validation. In such case, the token can represent blocks validation fees.

This involves that dedicated governance and regulation rules are associated to tokens.

Let's now consider the token legal status. The tokens introduced in the blockchain (coins…) may have different "kinds of value": they can either be related to usage they allow, as payment means or as investments (securities). According to the Howey test (money investment in a "common" enterprise where investors expect profits without having any impact in the enterprise success), most of the blockchain initial investment can be considered as securities, leading to different legal regulation depending on the country, only utility tokens allow being involved in the blockchain governance (i.e. the blockchain decisions).

1. 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…
2. Security tokens: are associated to money investment in a common enterprise in order to get profit.

3. Payment tokens are defined by the FINMA 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 the Initial Coin Offer. Tokens financial value can vary depending on the offer/demand rule. Note that depending on the project "utility" and on its community size speculation may occur.

2.3 Key governance and regulation requirements

After identifying the blockchain key concept and considering the impact of this distributed organisation to set governance and regulation rules, let's now focus on the key governance and regulation requirements.

Based on the blockchain key concepts and on the way this distributed organisation is managed, we can identify key governance and regulation requirements.

First of all, a blockchain provides a safe transaction support system, devoted to Peer to Peer exchanges. This technology can appear as the « missing transaction processing » element of the internet stack. This means that adapted governance and regulation requirements must be set to support large scale collaboration. As mentioned in the previous part, the different block validation strategies lead to various computing times and costs. Large scale development of the blockchain mechanism require improving the transaction validation efficiency.

Another important point is to consider the cyber risks. As blockchain provides a distributed trust mechanism, hacking affecting the core consensus mechanism must be considered. This leads to particular governance and regulation requirements related to the consensus mechanism, to the token status…

While setting regulation and governance requirements, a particular attention must be paid on the usage context and their particular requirements.

From the early Blockchain 1.0 to the last blockchain 4.0 developments, blockchain usages have been greatly increased. Different business areas make an heavy use of the blockchain technology. Of course, while Financial Technologies appear as a « natural » user of the blockchain due to the initial Bitcoin, collaborative networked organisations, such as distributed manufacturing, supply chains take also advantage of this distributed transaction management system. As a blockchain can store safely in a immutable way certified data, applications in the agriculture field (to support product trackability) or e-government are also increasing.

These new developments take advantage of the distributed transaction management to support distributed business transactions thanks to the generalized event-based organisation provided by the smart contracts. This can also be worthy used to integrate the large data set provided by IoT systems.

These data/event driven organisation supported by the smart contracts, the Blockchain services provided by the blockchain 2.0 and 3.0 provide a strong support on the Internet for opened collaborative and smart organisations.

This involves that dedicated regulations applying to these different usage contexts must be taken into account while developing blockchain governance and regulation.

Let's now introduce generic regulation constraints.

As an IT technology, Blockchain systems must fit regulation requirements regarding data protection, i.e. allowing confidentiality and privacy. Basically, the blocks and transaction stored in a blockchain can be accessed. So, this requirement involves that people using the blockchain must evaluate separately the requested protection level for the data that may be stored in a public ledger, define which extra encryption is required for sensitive information as those associated to manufacturing process, e-health records… before storing them in blocks. As far as private blockchain are concerned, appropriate access control on the ledger must be et to ensure that no unauthorized people can get any protected information.

Regarding the blockchain core organisation, parties are identified thanks to their private key without link to their real identity. This leads to a pseudonymous identification. This anonymity may be opposed to party identification requirements depending on the targeted usage.

Last but not least, tokens can be considered as securities. This involves that security regulation requirements must also be taken into account while developing an Initial Coin Offer or while using these tokens as payment means.

As a distributed transaction management system, a particular attention must be paid on the way responsibility is managed.

First, a blockchain is a distributed organisation so risks must be considered globally. A particular attention must be paid on the way each party involved in a blockchain manages security risks as one point of failure may affect the global system. Internal risks must also be considered although consensus methods have been designed to support distributed trust enactment: a group of validators can hack the blockchain and off-chain decision rules must be set to identify how to handle such a situation.

Second, a Peer to Peer transaction can be seen as an elementary contract between two (identified) parties. In blockchain 1.0, such a transaction can be associated to a payment while the smart contracts involved in blockchain 2.0 proposes to fix more complex rules. This technological development challenges for defining smart contract status: a « simple » data driven automated execution of a pre-defined transaction or a « legal » contract implementation. This « legal recognition » of smart contract depends also on the way parties' identity will be trusted.

Lastly, as an opened collaborative organisation, the core organisation of the blockchain provides an efficient integrity and non-repudiation mechanism as each transaction including the identification of the involved parties is stored in blocks and blocks stored in the different copies of the ledger. Due to this openness, a particular attention must be paid on the way privacy is managed as different legal context may be applied depending on the location of the blockchain node.

2.4 Conclusion

To sum up this presentation, blockchain technology has evolved from the early Blockchain 1.0 popularized by the Bitcoin to the last development turning blockchain technology into an IT component that can be integrated in various application developments. These different technologies rely on same core principles: a blockchain consists in a chain of trusted blocks, stored in a distributed ledger, each instance owning a copy of the ledger. Depending on the service provided by the blockchain system (payment, smart contract execution…), targeted usages, scalability and sustainability requirements on the blockchain system we have shown that the blockchain systems can be categorized depending on the technology they provide (i.e. the « blockchain version ») and on the potential access control on the blockchain system (permissionless vs permissioned blockchains).

Setting a blockchain involves that all parties approve the block validation strategy as this is the way trust is built in a distributed way. This refers to on-chain basic governance rules. As mentioned previously, off-chain decision rules must also be set to manage the distributed organisation, namely the way partners can join (or not) the blockchain system and how decision can be managed in case of internal hacks of the ledger (by felon validators).

As an IT technology, blockchain system must also fit legal constraints such as privacy, cyber risks management… Other constraints issued from the targeted application field or from the core blockchain principles (encryption) must also be considered. As the blockchain is a distributed system, a particular attention must be paid on the location of each stakeholder as regulation context depends on the hosting countries. Another important point of attention regarding regulation is associated to the token status: this can vary from a « technical object » for utility token to a security for crypto-currencies. In this last case, financial regulation must be considered.

3 PRACTICAL EXERCISES

This practical exercise shows how you can specify blockchain requirements. 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 the blockchain system you can propose to support such an ecosystem.

To solve this problem, you need to choose

- Ecosystem organisation
- Blockchain type / targeted usage
- Token status
- Key governance challenges
- Key regulation challenges

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

- Ecosystem organisation eans that you need to identify WHO are the participants and WHO are the users
- To address the blockchain type and targeted usage you need to identify Why the blockchain is introduced, What will be stored in the nodes
- To address the Token status, identify if payments / currencies are involved in the process
- Key governance challenges are focused on the ecosystem organisation (Who)
- Key regulation challenges are focused on the targeted usage (what is the target field, where are the participants and users)

Analysing the requirements shows that:

1. The ecosystem is associated to a mid-long term collaborative organisation: producers and suppliers are involved in a Just in Time supply chain, this means that they need to react fastly and know exactly what they can provide to each other. This collaborative organisation integrates all membrs of the supply chain
2. Product information associated to the transformation process must be stored in the blocks. This is a public information: clients must get access to it

3. Usage perimeter: the blocks are provided only by supply-chain members and clients can only read it.Consequently, an hybrid blockchain organisation is needed
4. The token ought to be an utility token as it does not represent any financial value
5. Key governance challenges are related to the ecosystem management, i.e. identifying / co-opting members
6. Regulation challenges are associated to the food product trackability. Depending on the type of product, extra production information (such as controlled temperature) can be added

4 CASE STUDIES

Case study : NFT based customer loyalty program

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 such a system.

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 is a permissioned blockchain?

A: A permissioned blockchain is designed for well-known and authorized participants, including validators.

Question and Answer No.2

Q: Can you explain why validators are trusted in Proof of Work consensus?

A: Trusting a block validation depends on the price “paid” by a validator. In Proof of Work systems, validators invest computing time and computing infrastructure leading to a significant cost.

Question and Answer No.3

Q: Can you explain why validators are trusted in Proof of Authority consensus?

A: Trusting a block validation depends on the price “paid” by a validator. In Proof of Authority systems, validators invest their reputation, in other words, malicious validation leads to a heavy cost regarding the reputation they will lose

Question and Answer No.4

Q: Can you explain the differences between utility and security tokens?

A: Utility tokens are technological assets used to grant an usage. They represent a kind of toll to use the system and allow their owner to take part in system governance. Security tokens are financial assets. They are used for payment or as investment to get profit.

Question and Answer No.5

Q: Is it possible to identify precisely parties using a blockchain?

A: Parties involved in blockchain transactions are identified thanks to their private key. As their “real world” identity is not proven, the blockchain users may be rather anonymous.

6 MULTIPLE-CHOICE QUESTIONS

Content example Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

Multiple Choice question No. 1

Q: Blockchain transactions

A: are P2P transactions

- Do not require any fees
- Are certified by a trusted party
- Are P2P transactions

Multiple Choice question No. 2

Q: Blockchain systems

A: may be public, private or hybrid

- Must be public systems
- Must be private systems
- May be public, private or hybrid systems

Multiple Choice question No. 3

Q: Which blockchain technology allows storing computerised transactions

A: Blockchain 2.0

- Blockchain 1.0
- Blockchain 2.0
- Blockchain 3.0
- Blockchain 4.0

Multiple Choice question No. 4

Q: Blockchain 1.0 systems provide

A: different non interoperable crypto-currencies

- A universal crypto-currency
- Different non interoperable crypto-currencies
- Software packages to support blockchain as a service

Multiple Choice question No. 5

Q: Blockchain 3.0 systems provide

A: Software packages to support blockchain as a service

- A universal crypto-currency
- Different non interoperable crypto-currencies
- Software packages to support blockchain as a service

Multiple Choice question No. 6

Q: Which block validation strategy is the worst regarding sustainability

A: PoW

- PoW
- PoS
- PoA

Multiple Choice question No. 7

Q: In a blockchain implementing a PoA validation strategy, validators

A: are certified parties and explicitly authorised to join the project

- Can join freely the ecosystem
- Can join the ecosystem, provided that they accept to invest
- are certified parties and explicitly authorised to join the project

Multiple Choice question No. 8

Q: Which validation strategy is the most efficient regarding the block validation QoS

A: PoA

- PoW
- PoS
- PoA

Multiple Choice question No. 9

Q: A security token

A: is a fiat currency

- Grant access to secured blockchain

- Is an authorisation token
- Is a fiat currency

Multiple Choice question No. 10

Q: Blockchain regulation

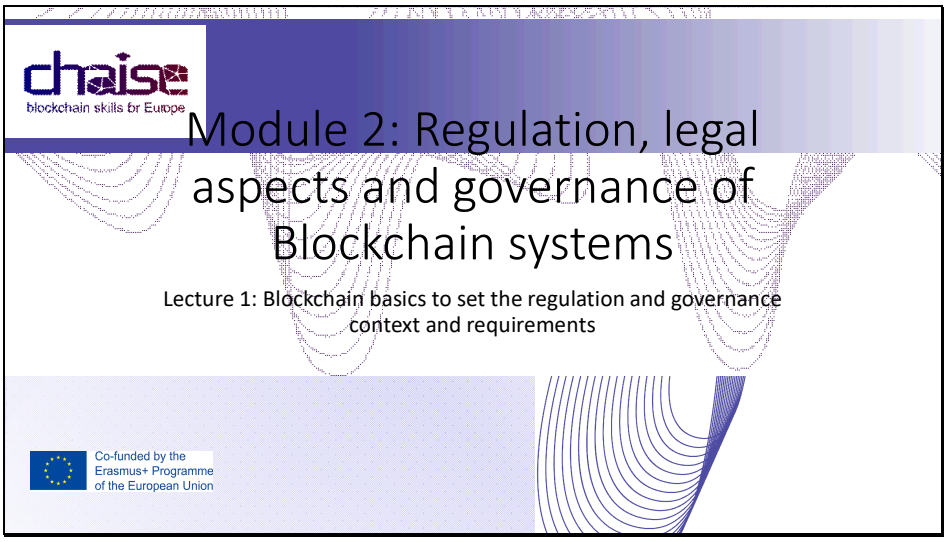
A: Depends on both location and target field

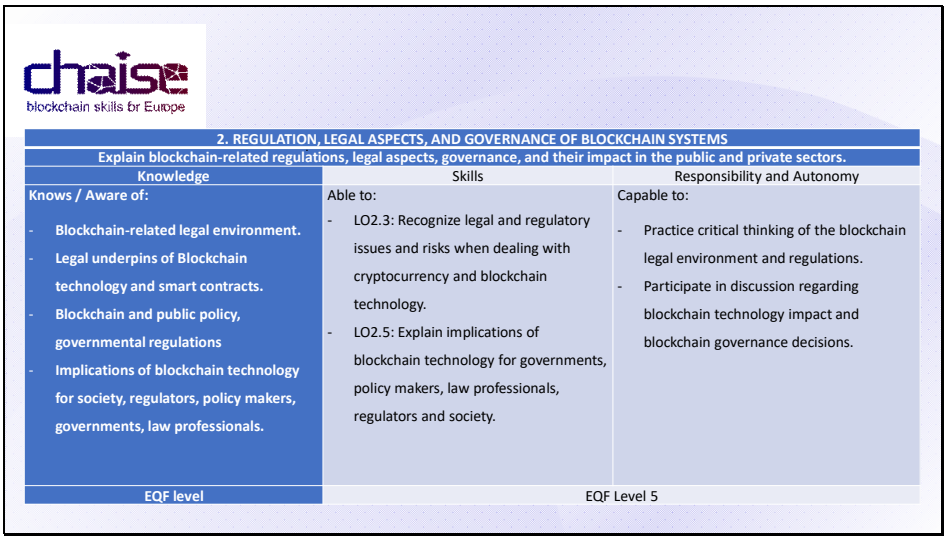
- Is universal
- Depends on the location
- Depends on the target field
- Depends on both location and target field

7 REFERENCES

- Mukherjee, P., Pradhan, C. (2021). Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology. In: Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C. (eds) Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_3
- https://vironit.com/a-blockchain-platforms-comparison/
- https://rubygarage.org/blog/best-blockchain-frameworks
- https://www.techtarget.com/searchcio/feature/Top-9-blockchain-platforms-to-consider
- Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, Suresh Chandra Satapathy, 2021. Blockchain Technology: Applications and Challenges. Springer, Intelligent Systems Reference Library. DOI: https://doi.org/10.1007/978-3-030-69395-4, ISBN: 978-3-030-69394-7

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: - Blockchain-related legal environment. - Legal underpins of Blockchain technology and smart contracts. - Blockchain and public policy, governmental regulations - Implications of blockchain technology for society, regulators, policy makers, governments, law professionals.	Able to: - LO2.3: Recognize legal and regulatory issues and risks when dealing with cryptocurrency and blockchain technology. - LO2.5: Explain implications of blockchain technology for governments, policy makers, law professionals, regulators and society.	Capable to: - Practice critical thinking of the blockchain legal environment and regulations. - Participate in discussion regarding blockchain technology impact and blockchain governance decisions.
EQF level	EQF Level 5	

How can you describe the blockchain governance and regulation requirements?

- Are all blockchain systems similar?
- Which blockchain characteristics impacts the governance rules?
- Who are the main actors? How do they interact with their environment?
- Which blockchain usages may involve regulation rules?

How can you describe the blockchain governance and regulation requirements?

- In this lecture you will
  - Identify key characteristics of blockchains that affect the internal governance
  - Learn how internal governance mechanisms are set
  - Identify how the ecosystem interact with its environment , leading to regulation requirements

chaise
blockchain skills for Europe

Learning objectives

Blockchain Key characteristics	Blockchain distributed organisation	Blockchain governance and regulation
Key concepts	Basic governance rules	Key requirements
Blockchain typology	Token usage status	Ecosystem organisation

Table of Content

- Blockchain key concepts
  - Distributed ledger
  - Blockchain typology
- Blockchain as a distributed organisation
  - Basic governance rule
  - Token status
- Governance and regulation
  - Key requirements
  - Ecosystem organisation
  - Key regulation principles
  Governance and regulation
- To conclude…

chaise
blockchain skills for Europe

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

Blockchain Key principles

- Blockchain = chain of blocks
  - A block stores
    - Transactions data
    - The previous block hash
  - A Merkle tree stores the blocks
    - Each block is signed with a hash
- Decentralized storage of the Merkle tree
  - Distributed ledgers
    - Safer storage
  - Common governance rule
    - How to trust the block validation process

A blockchain provides…

- A new service
  - To store P2P transaction
  - To manage trust
- As a service Blockchain has a cost…
- Blockchain is a distributed organization
  - Owned by community members => each member has to invest
  - No central authority => transaction fees are associated to the validation service
- Blockchain uses its own currency
  - Tokens
  - Need to exchange them with real world currencies

Blockchain access control

- Permissionless blockchain
  - Opened and shared ledgers
  - Free access for validators
  - Users are identified by their avatar
    - Anonymity
  - Public blockchain
- Permissioned blockchain
  - Authorized validators
  - Restricted access to the ledgers
  - Users are associated to well known identities
  - Used for private blockchain / consortium blockchain

Blockchain technology typology

Blockchain 1.0
Crypto-currency
Public blockchain
Validation paid by tokens

Blockchain 2.0
Include smart contract
Miners and developers are paid using tokens
Permissioned or permissionless systems

Blockchain 3.0
Blockchain middleware
Decentralized Apps
Towards XaaS model ?

Blockchain 4.0
"Easy to integrate" as a business support
Permission management
Block validation efficiency
Payment management

Cryptographic hashing techniques
Merkle tree

From blockchain characteristics to governance and regulation challenges

- Blockchain as a distributed organisation => governance rules
  - Block validation strategy
  - Validation payment
  - Access control (for private and hybrid blockchains)
- Blockchain as a transaction management system => regulation challenges
  - Users identification
  - Targeted business area
  - Token status: security or utility?

Table of Content

- Blockchain key concepts
  - Distributed ledger
  - Blockchain typology
- Blockchain as a distributed organisation
  - Basic governance rule
  - Token status
- Governance and regulation
  - Key requirements
  - Ecosystem organisation
  - Key regulation principles

  Governance and regulation
- To conclude…

Blockchain key principles: core governance rules

- Distributed oganisation
  - Multiple stakeholders
  - Trust management
  - Internal governance: block validation rule
- Proof of Work (PoW)
  - Block's hash is computed according to a mathematical challenge
    - Finding the "nonce" in a brute force way
  - Requires important computing resources and energy
    - Trust depend on the hardware investment and on the "consumed" computing resources
- Proof of Stake
  - Validator is randomly chosen according to the invested currency
  - Avoid heavy computation
    - Involves less speculation
- Proof of Authority
  - List of potential certified validators
  - Reputation mark

Blockchain extra governance rules depending on the targeted usage context

- Usage perimeter
  - Public => Permissionless blockchain
    - Identify potential users to identify the associated market
    - Community development strategy
  - Private => Permissioned blockchain
    - Who can participate
    - Cooptation mechanism
    - Costs sharing strategy
    - Restricted access to the ledger
  - Hybrid
    - Community based
    - Private part regarding the delivered services

Blockchain token?

- Cryptographic token
  - Digital asset
  - Access right
  - Set of rules stored in a smart contract
  - Issued and exchangeable on a blockchain
- Owners
  - Anonymity
  - Private cryptographic key stored in a wallet
- Tokens can be granted to miners
  - Reward for the block validation

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

Table of Content

- Blockchain key concepts
  - Distributed ledger
  - Blockchain typology
- Blockchain as a distributed organisation
  - Basic governance rule
  - Token status
- Governance and regulation
  - Key requirements
  - Ecosystem organisation
  - Key regulation principles

  Governance and regulation
- To conclude…

chaise
blockchain skills for Europe

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

chaise
blockchain skills for Europe

Key governance and regulation requirements

- Common requirements
  - P2P exchanges
  - Safe transaction system
- Internet opened environment to support large scale collaboration
  - Transaction validation efficiency
  - Internet security risk management
  - Complex ecosystem
- Different regulation and governance rules depending on the usages

Regulation requirements depending on usages : usage context

- Different business areas
  - Agriculture
  - Manufacturing and Supply chain
  - E-governement
  - Fin Tech
- Different distributed systems
  - From Business transaction
  - To IoT device integration
- Data / event driven organization
  - Smart contracts implement data dependent transaction
  - Opened ecosystem

Key regulation constraints depending on usages

- Different requirements
  - Data privacy / confidentiality
  - Parties identification vs anonymity
  - Crypto-assets value
- Responsibility management
  - Risks management
  - Contract status
- Opened Collaborative systems
  - Non repudiation
  - Data privacy

Table of Content

- Blockchain key concepts
  - Distributed ledger
  - Blockchain typology
- Blockchain as a distributed organisation
  - Basic governance rule
  - Token status
- Governance and regulation
  - Key requirements
  - Ecosystem organisation
  - Key regulation principles
  - Governance and regulation
- To conclude…

chaise
blockchain skills for Europe
Co-funded by the Erasmus+ Programme of the European Union

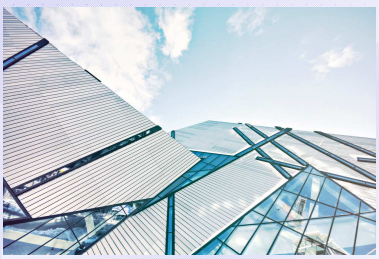
To conclude…

- Different blockchain technologies
  - Depending on the provided service
  - Different internal organisation
- Basic governance rules
  - To mange ecosystem internal interaction
    - Block validation
    - Access control
  - To manage the distributed organsation
- Regulation depends on
  - Country
  - Blockchain targeted applications
  - Token status

chaise
blockchain skills for Europe
Co-funded by the Erasmus+ Programme of the European Union

Resources

- Mukherjee, P., Pradhan, C. (2021). Blockchain 1.0 to Blockchain 4.0—The Evolutionary Transformation of Blockchain Technology. In: Panda, S.K., Jena, A.K., Swain, S.K., Satapathy, S.C. (eds) Blockchain Technology: Applications and Challenges. Intelligent Systems Reference Library, vol 203. Springer, Cham. https://doi.org/10.1007/978-3-030-69395-4_3
- https://vironit.com/a-blockchain-platforms-comparison/
- https://rubygarage.org/blog/best-blockchain-frameworks
- https://www.techtarget.com/searchcio/feature/Top-9-blockchain-platforms-to-consider
- Sandeep Kumar Panda, Ajay Kumar Jena, Santosh Kumar Swain, Suresh Chandra Satapathy, 2021. Blockchain Technology: Applications and Challenges. Springer, Intelligent Systems Reference Library. DOI: https://doi.org/10.1007/978-3-030-69395-4, ISBN: 978-3-030-69394-7



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