BLOCK START

D5.8: Policy Recommendations – 2nd version

07/2021

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 828853.

Work Package	WP5
Document Reference	BS-WP5-D5.8-Policy Recommendations-2nd-version
Document Type	Report
Author	CIVT
Contributor(s)	BRPX, F6S
Delivery Date (DoA)	31/07/2021
Actual Delivery Date	30/07/2021
Abstract	Report detailing desk research and results from the policy webinars, the existing framework conditions and the recommendations given the project learnings

Document Revision History			
Date	**Version**	**Contributor(s)**	**Description**
23/07/2021	v1.0	CIVT	First version
30/07/2021	Final	BRPX, CIVT, F6S	Final version including review by BRPX, CIVT and F6S

Dissemination Level	
PU	Public

BlockStart Consortium			
Participant Number	**Participant Organisation Name**	**Short Name**	**Country**
1	Bright Development Studio, S.A.	BRPX	PT
2	UAB CIVITTA	CIVT	LT
3	F6S Network Limited	F6S	UK

Funding Scheme: Coordination and Support Action (CSA) ● Theme: H2020-INNOSUP-03-2018

Start date of project: 01 September, 2019 ● Duration: 30 months

Table of contents

List of figures

List of Abbreviations and Acronyms	
DLT	Distributed Ledger Technology
DeFi	Decentralized Finance
CeFi	Centralized Finance
Q	Question
M	Million
SME	Small and Medium-sized Enterprise
AML	Anti-Money Laundering
CFT	Combating the Financing of Terrorism
KYC	Know Your Customer
EDPB	European Data Protection Board
EC	European Commission
MiCA	Markets in Crypto-assets
ICO	Initial Coin Offering
STO	Security Token Offering
IATBA	International Association for Trusted Blockchain Applications
DG	Directorate-General
EUIPO	European Union Intellectual Property Office
R&I	Research and Innovation
EIC	European Innovation Council
EFTG	European Financial Transparency Gateway
DG FISMA	Directorate-General for Financial Stability, Financial Services and Capital Markets Union
ESMA	European Securities Markets Authority
IDiLeTech EP	Impact of Distributed Ledger Technology in European Policymaking
EMD2	E-money Directive
SSI	Self-sovereign identity
DIDs	Decentralized identifiers

1. Introduction

As interconnectivity of the world is constantly increasing, a vast set of opportunities can emerge from blockchain as a technology that could enable parties with no particular trust in each other to exchange any kind of digital assets (money, contracts, land titles, medical and educational records, services or goods) on a peer-to-peer basis with fewer to no intermediaries.

Blockchain / DLT can bring many opportunities, such as, allow individuals, firms, public organisations and other entities to validate transactions and update records in a synchronised, transparent and decentralised way. These new mechanisms for creating and managing data can be impactful across sectors – for instance, when it comes to increasing efficiency and automating processes, reducing costs or spurring new organisational and business models. Possible benefits of transparency, security and increased trust are now apparent for a range of applications and use cases where it is key to move from closed to more open systems.

The rise of blockchain technology-based solutions has presented a lot of opportunities for making processes more trustworthy, safe and potentially more effective. However, alongside the promises of the technology that aimed to revolutionize the current status quo, came a lot of challenges. How do you regulate applications that pose fundamental challenges to the way you do business? Can current regulatory institutions and instruments be adapted or does it require a completely different framework?

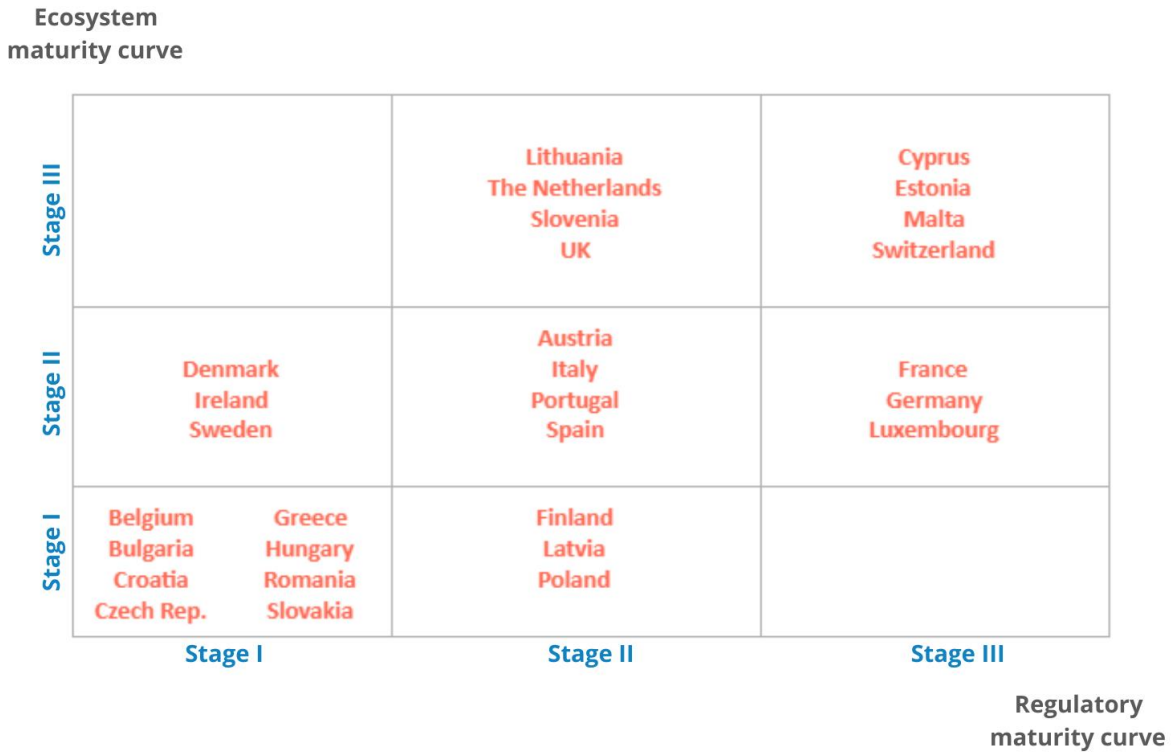
To answer these questions the analysis and insights presented in this document have been collected through a combination of desk research, discussions with the regulators through policy webinars organized by the BlockStart team. The information collected during the project will be used extensively to facilitate the development of a compelling regulatory framework and government support activities to SMEs.

2. Overview of the legislative context

Despite the many benefits of blockchain / DLT currently there are lots of challenges that come with it. Core technical bottlenecks remain unresolved which, depending on the type of blockchain, can include scalability and performance, interoperability, transaction costs, high energy consumption and the protection of personal, sensitive or confidential data. Regulatory uncertainties over the formal status of blockchain applications are threatening and affecting the pace of the sustainable technology development for firms and other organisations either piloting blockchain or interested in its deployment which can be considered as a high-risk business matter.

According to the EU Blockchain Ecosystem Developments Report the regulatory and legal framework was identified as a large issue[1]. The regulation is still developing and very few countries in the EU have set concrete rules to guide the blockchain industry. Cyprus, Estonia, Marta and Switzerland are front-runners in this respect, but other regional laws or an EU-wide framework does not currently exist. So, it is very important to investigate various regulatory aspects in the field of blockchain / DLT since the majority of European countries are in the stage 1 of regulatory and ecosystem maturity (see Figure 1).

Figure 1. Ecosystem and regulatory maturity stages of European countries



Source: EU Blockchain Observatory and Forum: EU Blockchain Ecosystem Developments Report

As the figure above suggests, on a path towards harmonizing the regulatory and policy frameworks EU member states are currently at different maturity levels in terms of regulatory and ecosystem development. Each country can be broadly grouped in one of three stages of maturity in each dimension of each maturity curve (regulatory and business):

Regulatory maturity curve measures the degree of top-down support provided by national or regional government:

[1] A Thematic Report Prepared By The European Union Blockchain Observatory & Forum "EU Blockchain Ecosystem Developments", 20 November 2020, https://www.eublockchainforum.eu/reports

Stage I of the regulatory maturity, where no specific blockchain-related legislation exists.

Stage II of the regulatory maturity, where the state has shown signs of significant involvement with the field, through a combination of adoption of wider regulatory schemes (for example, related to Know Your Customer (KYC) / Anti Money Laundering (AML), but also explicitly touching upon crypto assets, such as regulation of alternative forms of financing, Initial Coin Offerings (ICOs), Security Token Offerings (STOs) or through other specific measures, which might include government-sponsored studies (for example, taxonomies of virtual assets as far as applicable existing regulation is concerned) or government-sponsored pilot applications of blockchain in the public sector. An established framework for the taxation of digital currencies and digital assets is another characteristic of countries that fall under Stage II.

Stage III of the regulatory maturity, where either specific legislation for blockchain or crypto assets have been voted on or published and / or the government has announced a national strategy / vision specific to blockchain (or for new technologies explicitly addressing blockchain). Regulatory sandboxes, innovation hubs and other initiatives that allow blockchain, fintech and other firms to pilot novel implementations, as well as the involvement of the banking sector, are also characteristics of countries in Stage III.

Ecosystem maturity curve measures the degree of bottom-up development of the local ecosystem in each country, as evidenced through three main indicators: presence of a local business / startup ecosystem; number of blockchain-related formal education and academic research initiatives; number of user-driven communities around blockchain or virtual assets. Countries were grouped into three broad categories:

Stage I of the ecosystem maturity, where there is evidence of sizeable and dynamic initiatives in none or one of the three indicators (business, academia, communities).

Stage II of the ecosystem maturity, where there is evidence of sizeable and dynamic initiatives in at least two of the three indicators.

Stage III of the ecosystem maturity, where there is evidence of sizeable and dynamic initiatives in all three indicators.

29 European countries were analysed according to the 3x3 matrix presented in Figure 1. It is worth noticing that naturally the borders between categories are by definition porous and countries may not always objectively belong strictly to one of the matrix categories. It must also be stressed that this is a fast-evolving space, so that all countries are expected to gradually move from the bottom left to the top-right part of the matrix. Notwithstanding these, the insights of the EU Blockchain Ecosystem Report and the assessment matrix was a helpful instrument in assessing the status of the European blockchain ecosystem at the end of 2020.

The meaning of ecosystem and regulatory maturity could be briefly explained as an existing regulatory framework with the holistic approach when the measures of empowerment and support of blockchain

/ DLT development are taken into account in terms of innovation and competition while mitigating the risks.

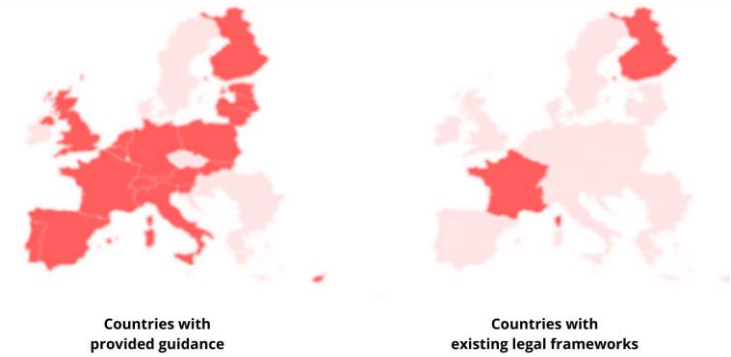
2.1 Status of regulatory framework and guidelines in the EU policy context

In this section the status of regulatory frameworks and guidelines in the EU policy context is presented. As stated in the previous section the regulatory maturity curve of blockchain differs in many countries depending on the support provided by national or regional governments. While there are no regulatory frameworks in some countries (Bulgaria, Croatia, Denmark, etc.), some other countries are way ahead in creating legal frameworks and regulation of blockchain (Cyprus, Estonia, Switzerland, and Malta among them). The European Commission's shared actions on the regulation of crypto-assets taken in the year 2020 represent the first concrete action in this area. The regulatory context of digital assets in finance is of utmost importance because this is blockchain's most developed area of use and so holds lessons for the technology's future also in other sectors.

2.1.1 Current situation

Most European countries do not yet have a specific and holistic regulatory or legal framework for virtual assets. However, there is a growing number of countries that have already adopted or are developing such a legal framework and / or have announced guidelines for the legal treatment of virtual assets. An overview of the countries with existing legal frameworks and provided guidance for virtual currencies in Europe is shown in the following figure.[2]

Figure 2. An overview of the European countries' *current regulatory situation*



Source: EU Blockchain Observatory and Forum: EU blockchain Ecosystem Developments Report

[2] A Thematic Report Prepared by The European Union Blockchain Observatory & Forum "EU Blockchain Ecosystem Developments", 2020, https://www.eublockchainforum.eu/reports

Where no specific regulatory framework exists, member states have adopted taxonomies or characterizations of virtual assets to identify the most applicable existing regulatory treatment in each case. For example, the position of the Bank of Lithuania states that financial market participants (FMP) cannot provide services associated with virtual assets, yet in certain cases companies wishing to use blockchain technology must purchase a small part of virtual assets. The current position of the Bank of Lithuania does not necessarily imply that companies cannot use a public blockchain technology. Holding of virtual assets for the purposes of using the technology is not considered to be virtual assets related activities or services. FMPs may hold a small quantity of virtual assets for the purposes of using blockchain technology in their activities; nevertheless, provision of services to customers should be expressly separated from virtual assets.[3]

It should be mentioned that even though no specific legal framework exists for virtual assets in most of the European countries, the laws pertaining to anti-money laundering and countering terrorist financing provisions are applied to virtual currencies. As far as taxation in European countries is concerned, in most jurisdictions no specific tax laws on the taxation of virtual currencies exist and their tax treatment is based on general principles and guidance issued by the national tax authorities.

2.1.2 Future actions

On September 24, 2020 the European Commission announced legislative proposals on crypto assets or a new Digital Finance package to draw on the possibilities offered by crypto-assets, while mitigating risks for investors and financial stability that involves a proposal for regulation on markets in crypto assets, which creates a pan-European regulatory regime for crypto assets and related services, as well as a pilot regime for market infrastructures based on distributed-ledger technologies, offering a safe space for testing innovative technologies around DLT-based financial market infrastructures in the European Union. One of the main objectives of the proposed legislative framework is to provide a sound legal framework for all crypto assets not currently covered by the existing financial services legislation, thereby providing the necessary legal certainty required within the European Union for the development of the crypto-asset markets.

The new Digital Finance package by European Commission including Digital Finance and Retail Payments Strategies and legislative proposals on crypto-assets and digital resilience[4] are listed below.

A Digital Finance Strategy: towards a European financial data space - new ways of channelling funding to SMEs - better financial products for consumers. Today's Digital Finance Strategy aims to make financial services in Europe more digital and to promote responsible innovation and competition among financial services providers in the EU. It will reduce fragmentation of the digital single market so that consumers can access financial products across borders and fintech start-ups can scale up and

[3] Bank of Lithuania position on virtual assets and initial coin offering reflects changing market realities, 2 February 2019, https://www.lb.lt/en/news/bank-of-lithuania-position-on-virtual-assets-and-initial-coin-offering-reflects-changing-market-realities

[4] Digital Finance Package: Commission sets out new, ambitious approach to encourage responsible innovation to benefit consumers and businesses, 24 September 2020, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684

grow. It will ensure that EU financial services rules are fit for the digital age for applications such as artificial intelligence and blockchain. Data management is also at the heart of today's strategy. In line with the Commission's broader Data Strategy today's actions aim to promote data sharing and open finance while maintaining the EU's very high standards for privacy and data protection. Finally, the strategy aims to ensure a level playing field for financial services providers, be they traditional banks or technology companies: same activity, same risks, same rules.

A Retail Payments Strategy: modern and cost-effective payments. The strategy aims to provide European citizens and businesses with safe, fast and reliable payment services (which potentially could be executed using blockchain / DLT technology). It will make it easier for consumers to pay in shops and carry out e-commerce transactions safely and conveniently. It aims to create a fully integrated retail payments system in the EU, including instant cross-border payment solutions. This will facilitate payments in euros between the EU and other countries. It will encourage the emergence of domestic and pan-European payment solutions.

Legislative proposals on crypto-assets: seizing opportunities and mitigating risks. For the first time (on September 24th, 2020) the Commission proposed new legislation for crypto-assets (a digital representation of value or rights that can be stored and traded electronically). The Markets in Crypto Assets Regulation (MiCA) will encourage innovation while preserving financial stability and protecting investors from risk. It will provide legal clarity and certainty for issuers and providers of crypto-assets. The new rules will allow operators authorised in one Member State to offer their services throughout the EU ("passporting"). Safeguards include capital requirements, custody of assets, a mandatory complaints procedure available to investors, and investor rights against the issuer. Issuers of significant asset-backed crypto assets (so-called global "stablecoins") would be subject to more stringent requirements (e.g., capital, investor rights and supervision).

The Commission also proposed a pilot regime for market infrastructures seeking to trade and settle transactions in financial instruments in the form of crypto-assets. The pilot regime represents a so-called "sandbox" approach - or controlled environment - that allows temporary exemptions from existing rules to allow regulators to gain experience with the use of distributed ledger technology in market infrastructures while ensuring they can manage risks to investor protection, market integrity and financial stability. The intention is to allow firms to test and learn more about how existing rules perform in practice.

Legislative proposals on digital operational resilience: closing the door to cyber attacks and enhancing oversight of outsourced services. Technology companies are becoming increasingly important in finance, both as IT providers to financial firms and as providers of financial services themselves. The proposed Digital Operational Resilience Act (DORA) seeks to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyber-attacks and other risks. The proposed legislation will require all firms to ensure that they can withstand all types of disruptions and threats related to Information and Communication Technology (ICT). The proposal also introduces an oversight framework for ICT providers, such as cloud computing service providers.

In addition, the proposed DORA framework aims to encourage and promote innovation related to crypto-assets and the wider use of DLT in a proportionate and secure manner. Another objective is to ensure an appropriate level of consumer and investor protection and market integrity, as well as to ensure financial stability. One of the important aspects of the proposed framework for crypto-assets is that European Commission distinguishes between those crypto-assets that are already regulated by EU law and other crypto-assets, thereby creating a safe environment for innovation by maintaining financial stability and protecting potential investors. No changes are proposed for crypto-assets already subject to existing legislation. However, European Commission proposes a pilot regime for market infrastructures to test trading and settlement processes using crypto-assets, allowing market participants and regulators to gain experience with the use of DLT exchanges.

Following increased governments' engagement, the introduction of relevant regulation, the promotion of research and, in certain cases, regulatory sandboxes and innovation hubs, an increasing number of initiatives exploring the full range of blockchain applications outside the financial services sector are observed. The related key challenges and potential solutions (EU actions) are provided in the following section.

3. Key industry challenges and policy recommendations

While acknowledging a number of opportunities and risks, there is a need for enhanced regulatory capacity, including technical expertise, the development of a sound legal framework and the promotion of shared and inclusive governance of the blockchain / DLT.

Policymakers and regulators need to progress in assessing whether existing policies and laws are fit for purpose or if new frameworks will be required. According to the desk research, the intensive discussions in the blockchain / DLT regulation scene include the following topics:

- Blockchain and GDPR
- Standartization
- Consumer and investor protection - identity management
- Validity of smart contracts
- Notary - legal recognition of signatures
- Enforcement of anti-money laundering requirements
- Applicable jurisdictions (including cross-border jurisdiction)
- Legal classification and taxonomy of tokens and digital programmable Euro

More detailed descriptions as well as potential EU actions of the aforementioned matters will be provided in the following sections.

3.1 Blockchain and GDPR

There is great intensity between the very nature of blockchain technology and the overall structure of the General Data Protection Regulation (GDPR), and according to ongoing discussions in the European Parliament, currently there is a lack of legal certainty as to how various elements of European data protection law ought to be applied to blockchain[5].

Basically, this uncertainty has two determining factors. Firstly, it has been seen that very often the very technical structure of blockchain technology as well as its governance arrangements stand in contrast with legal requirements. Secondly, it has also been observed that trying to map the regulation to blockchain technologies reveals broader uncertainties regarding the interpretation and application of this legal framework. The GDPR is legislation based on broad general principles. This brings flexibility and adaptability advantages in the age of fast technological change, but also has downsides, at times for instance making it difficult to determine with certainty how a specific provision ought to be applied in a specific context.

One of the most discussed issues concerns potential conflicts between blockchain and the GDPR right to data erasure, best known as 'the right to be forgotten'. The potential need to identify and contact all the necessary nodes with a request to delete or even rectify data ('right to amendment') might not be feasible in reality. Also, any changes in a tamper-resistant database may erode the participants' trust in the blockchain itself and lend it to suspicions of tampering and interference.

Potential EU actions

It is unclear how storing personal data on blockchain exactly fits into the present regulatory environment. The immediate problem is that the precise meaning of 'erasure' is left undefined. While crafting the text regulators likely had traditional databases in mind that allow hard drives to be wiped clean and database entries deleted. The tamper-proof nature of blockchain makes a 'clean-wipe' of data difficult or sometimes even impossible. Instead, data can be rendered inaccessible making it effectively erased; however, data protection officers could take issue as it may not fit their interpretation of understanding the data 'erasure' meaning.

Regulatory guidance could as a matter of fact provide more legal certainty compared to the current status quo. This could take the form of various regulatory initiatives. As one of the ways, supervisory authorities could coordinate through the European Data Protection Board (EDPB) to draft specific guidance on the application of the GDPR to blockchain technologies at supranational level, preventing the risk of fragmentation that would result from numerous independent initiatives[6].

[5] Blockchain and the General Data Protection Regulation, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf

[6] STOA Options Brief, Blockchain and the General Data Protection Regulation, 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445(ANN1)_EN.pdf

3.2 Standardization

Blockchain technology can only realize its potential through cross-industry and cross-domain standardization and certification. Standards can help guide and align activities to promote the development of blockchain technology. Trust in the technology across all stakeholder domains would be enhanced but most importantly, usability and operational efficiency are significantly improved through interoperability, leading to reduced friction, cost reductions and the avoidance of unwanted lock-in effects. At the same time this leads to significant reputation gains and thus increases technology acceptance.

Technical standards should include smart contract oracles, which are trusted entities that import external data into the blockchain and are therefore a critical part of a blockchain system. Standards should be set to ensure technical interchangeability, meaning that smart oracles can feed data into the blockchain system regardless of the blockchain technology used. In addition, self-authentication should be standardized and certified, i.e., technical solutions that can detect that the location of the device is the correct one and has not been tampered with to ensure integrity and trust across domains.

The current pack of ISO Standards[7]:

- ISO 22739 Blockchain and distributed ledger technologies – Vocabulary;
- ISO/TR 23244, 'Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations';
- ISO/TR 23455, 'Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems';

is a great step towards standardization, however the wider approach to standard application and implementation is needed.

Potential EU actions

Overall, standards play an essential role in terms of blockchain technology adoption. They will lead to interoperability, reduce the risk of fragmentation, avoid lock-in effects, create trust in privacy and security aspects, establish a common language and set clear governance rules. Therefore, they will increase adoption and investment. Standards are the basis for the necessary network effects for technological breakthroughs and drive innovation rather than fragmentation and reinventing the wheel.

Regulators should quickly push for overarching standards, as the current development of diverse and competing standards by different stakeholders will lead to fragmentation[8].

[7] ISO 35.030 IT security including encryption: https://www.iso.org/ics/35.030/x/

[8] Blockchers, Consultation on regulatory policy, 2021, https://blockchers.eu/wp-content/uploads/2021/05/D4.5_Consultation-on-regulatory-policy-changes-regarding-DLT.pdf

3.3 Consumer and investor protection - identity management

The future of identity is digital. The Internet has fundamentally changed the way information is transmitted. However, the current solution to online identity is both precarious and archaic. As digital becomes increasingly ubiquitous, a continuation of the status quo could spell disaster. The implication is clear. A secure online identity layer has become an important but missing infrastructure for modern society.

Accessing online services or conducting online transactions requires citizens to disclose relevant information or provide proof of identity. Citizens are typically required to provide financial and personal information that is stored on centralised or government-controlled platforms or databases. Many such databases are subject to serious security problems, as evidenced by news of widespread security breaches exposing users' personal data.

In this respect, the question of who processes, stores and holds such data, how and for what purposes is at the heart of recent and ongoing European regulatory initiatives under the Digital Single Market strategy.

These include, inter alia, the draft Regulation on a framework for the free flow of non-personal data in the EU, the GDPR (Regulation (EU) 2016/679) and the Regulation on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (Regulation (EU) No 910/2014).

One of the main findings in the Frontiers in Blockchain article "Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual" is that the management of digital identity is transforming from a purpose-driven necessity toward a self-standing activity that becomes a resource for many digital applications. In other words, whereas traditionally identity is addressed in a predominantly sectoral fashion whenever necessary, new technologies transform digital identity management into a basic infrastructural service, sometimes even a commodity. This coincides with a trend to take the "control" over identity away from governmental institutions and corporate actors to "self-sovereign individuals," who have now the opportunity to manage their digital self autonomously[9].

EU actions

It is unclear exactly how storing personal data on the blockchain fits into the current regulatory environment and the need for a robust identity system has been already recognized by European Commission. Commission President Von der Leyen announced in her September 16, 2020 speech: "<...> We want a regulatory framework that puts people at the center. Algorithms must not be a black box and there must be clear rules if something goes wrong".[10] In January 2021 European Commission proposed a trusted and secure Digital Identity for all Europeans - a framework for European Digital Identity which will be available to all EU citizens, residents and businesses in the EU. Citizens will be

[9] Ibid

[10] European Commission, "State of the Union Address by President von der Leyen at the European Parliament Plenary", 2020. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

able to prove their identity and share electronic documents from their European Digital Identity wallets with the click of a button on their phone[11]. However, there is no requirement for Member States to develop a national digital ID and to make it interoperable with the ones of other Member States, which leads to high discrepancies between countries. The current proposal will address these shortcomings by improving the effectiveness of the framework and extending its benefits to the private sector and to mobile use.

3.4 Validity of smart contracts

Smart contracts are currently only feasible or applicable under limited and strictly circumscribed conditions, for example, when there is no need for dispute resolution or when there is a reliable oracle that provides accurate information. Relevant challenges may arise when considering the possibilities for people and organisations to create their own rule systems or smart contracts as a kind of automated private ordering framework or lex cryptographia that can bypass court rules and operate across countries in the near future.

In most cases smart contracts are related to legal contracts in some way: the former may constitute a part of a legal contract, an entire contract or be used to automate contract performance. Meanwhile, the question of whether modern contract law applies to smart contracts is rather controversial, as smart contracts were originally conceived as relying only on technical rules embedded in the blockchain and were considered as self-sufficient instruments capable of solving various problems that may arise in practice. However, practice has shown that technical regulation often fails to cope with the problems that can be faced when using smart contracts, confirming the need for legal regulation. Although smart contracts have many technical features, they do not make the application of contract law regulations completely impossible. Thus, what modern contract law needs is a set of specific rules applicable to the practice of smart contracting.

Just as there are many limits to freedom of contract in general, there will be many limits in contract law and regulation on the autonomy and self-enforcement of smart contracts. Smart contracts do not exist in a legal vacuum just as cyberspace is not cut off from the real world.[12]

Potential EU actions

Many jurisdictions around the world introduce regulatory frameworks which provide assurances regarding due diligence on individuals, entities and the financial operations surrounding a regulated entity's activities.

It seems clear that there is a need to create a common international regime on the systems of accreditation of the identity of persons participating in blockchain and smart contracts. An international digital identity system should also capture some essential attributes such as age and

[11] European Commission, "Commission proposes a trusted and secure Digital Identity for all Europeans", 2021, https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[12] Bird&Bird, "Blockchain 2.0, smart contracts and challenges'', https://www.twobirds.com/~/media/pdfs/in-focus/fintech/blockchain2_0_martinvonhallergroenbaek_08_06_16.pdf

eligibility to be part of a contract.[13]. Although the use of asymmetric cryptography systems provide security and strengthen the authenticity of the transaction, it will be necessary to consider whether or not some identity systems on public blockchain platforms can be admitted by the courts in the event of a dispute. For this reason, it seems foreseeable that the blockchain systems eventually prevailing in the market and in market transactions will be those that are private and authorised, i.e., those where a legal entity manages and monitors the access of users, thus guaranteeing their identity, as opposed to the inherent risks and lack of transparency of public Blockchain platforms.[14]

3.5 Notary - legal recognition of signatures

The foundation for digital trust through legally recognized e-signatures has been laid with the eIDAS Regulation, Electronic Identification, Authentication and Trust Services Regulation, which aims to provide a predictable framework for e-signatures that includes electronic identification and electronic trust services within the European market by establishing a single set of standards. Binding basic principles are introduced, such as cooperation on eIDs and trust services and cross-border acceptance of ID cards. There are three levels of legal security of signatures / eSeals under eIDAS: simple, advanced and qualified. The qualified signature is the highest level of signature and corresponds to the handwritten signature in legal transactions.

The EU Directive 199/93/EC was the first wide-scale e-signature legislation to take effect in the European Union. All member states were required to be in compliance by July of 2001. The Directive was repealed by the electronic IDentification, Authentication and trust Services (eIDAS) regulation on 1 July 2016[15]. Decentralized identity on a blockchain system supports the essence of eIDAS in various aspects. However, as eIDAS was designed with a more centralized structure in mind, some challenges need to be further clarified. Additionally, there is a lack of legally binding digital signatures across entities and domains.

Potential EU actions

In order to create an environment of trust in which transactions on a blockchain system can be executed in a legally secure manner, clarification of the requirements for achieving a qualified signature is needed, i.e., a legally binding digital signature across entities and domains under eIDAS would be essential. Within decentralized identity systems on a blockchain, many aspects are already in line with the spirit of eIDAS. In particular, the structure of the self-sovereign identity (SSI) with its decentralized identifiers (DIDs) that uniquely identify all subjects (a person, organization, thing, data

[13] University of Twente, Djuri Baars, Towards Self-Sovereign Identity using Blockchain Technology. https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

[14] European Bank, Smart contracts - Legal framework and proposed guidelines for lawmakers, 2018, https://www.ebrd.com/documents/legal-reform/pdf-smart-contracts-legal-framework-and-proposed-guidelines-for-lawmakers.pdf

[15] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093

model), combined with verifiable assertions (a piece of information that describes qualities or properties) meets many requirements[16].

3.6 Enforcement of anti-money laundering requirements

The inadvertent use of the banking system for money laundering activities is a key challenge for the financial services industry. In response, regulators have introduced anti-money laundering (AML) regulations to detect and prevent such activities. Compliance with these regulations requires banks and financial institutions to implement an effective compliance system with appropriate tools and procedures. This in turn requires firms to build an effective business case for the right compliance system, equipped with the necessary skills and the latest technology tools.

Money launderers will always find new ways to use banks for illegal activities. Timely detection of money laundering activities is the biggest challenge in implementing an effective AML program. Currently, several innovative technology-based tools and products are available to detect, track and prevent money laundering. Although these technology tools will not completely eliminate money laundering, they will bring it under control to a large extent and financial institutions should proactively seek to implement them sooner rather than later.

Change is constant in the financial industry. With the digital revolution and the added complexity of the global pandemic, firms around the world are being restructured and reshaped. The same is true for compliance and regtech. As a result of the new regulations that have come into effect over the past year and the new policies that are already on the horizon.

EU actions

EU anti money laundering directives are issued periodically by the European Parliament to be implemented by member states as part of domestic legislation. The European anti-money laundering directives (AMLD) are intended to prevent money laundering or terrorist financing and establish a consistent regulatory environment across the EU. This is done by addressing the emerging money laundering and terrorist financing typologies, helping to close AML compliance gaps.

When the EU issues an anti-money laundering directive, it also sets an implementation date by which appropriate AML / CFT legislation must be in place within member states. Since implementation periods can last several years, new money laundering and terrorism financing threats may emerge during that time: accordingly, the EU issues new anti-money laundering directives regularly to reflect changes in criminal methodology and in AML / CFT best practices.

[16] Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations W3C Candidate Recommendation Draft, 2021, https://www.w3.org/TR/did-core/

On 19 June 2018 the 5th anti-money laundering Directive (Directive (EU) 2018/843), which amended the 4th anti-money laundering Directive, was published in the Official Journal of the European Union. The Member States had to transpose this Directive by 10 January 2020[17].

These amendments introduced substantial improvements to better equip the Union to prevent the financial system, including players using blockchain / DLT technologies, from being used for money laundering and for funding terrorist activities.

3.7 Applicable jurisdictions (including cross-border jurisdiction)

Nowadays digital business models, especially blockchain-based solutions, are inherently transnational in nature. Companies operating across borders need legal certainty with regard to litigation. When it comes to issues of responsibility and liability, questions remain with this still young and immature technology. Since the nodes of a blockchain that form a consensus within the network can be spread across the globe, the regulatory challenges become even more complicated.

This is particularly the case when it comes to highly regulated sectors such as financial services. In this sector there is traditionally some sort of central counterparty, which is often regulated. Within a particular system or process this central party is accountable and takes responsibility for providing services to all other participants through a contractual framework underpinned by the legal and regulatory structure. An example of this would be the role of a central bank or other institution in clearing and settlement processes.

In many blockchain use cases, however, there is no such centralized party that takes responsibility for providing services or controls the associated data sets. Instead, each party in the blockchain network holds a copy of the data, rather than relying on a single centralized party to hold and maintain a master copy. Blockchain technology is being used, for example, to simplify cross-border payments by eliminating the need for remittances to pass through multiple parties (with their associated fees) before reaching their destination[18]. While such decentralization can bring benefits, it also presents legal and regulatory challenges when there is no central party that is responsible and can be held accountable[19].

Potential EU actions

As countries and regulations differ, the cash flow routes vary. In this massive payment market cross-border payment faces risks of frauds, trading risks and capital risks that require solutions by fintech innovation. From the perspective of blockchain coalition, the establishment of a theoretical

[17] Anti-money laundering (AMLD V) - Directive (EU) 2018/843, https://ec.europa.eu/info/law/anti-money-laundering-amld-v-directive-eu-2018-843_en

[18] Financial Times, Ripple and Swift Slug It Out Over Cross-Border Payments, 2018, https://www.ft.com/content/631af8cc-47cc-11e8-8c77-ff51caedcde6

[19] EM Compass, Blockchain and Associated Legal Issues for Emerging Markets, 2019, EMCompass-Note-63-Blockchain-and-Legal-Issues-in-Emerging-Markets.pdf

framework and model for cross-border payment, exploring the prospect and challenges of digital currency and cross-border payment would be an essential step[20].

A typical barrier to the EU internal market development is still related to the definition of applicable jurisdiction to cross-border activities. Blockchain offers a new technical environment to exchange value. A clear regulatory framework is needed that addresses the issue of cross-border jurisdiction.

3.8 Tokens and digital programmable Euro

Tokens can be defined as a programmable representation of real or virtual assets, including all the rights and obligations they contain, that are collectively managed in a ledger that tracks and displays the universal status of ownership. This is an essential component of a blockchain system, as all interactions should take place on the blockchain to enable the synchronization of the flow of goods, money and invoices. This would eliminate the current structure of separate silos. Tokens are the enablers of such a synchronized system as they can provide economic value.

'Digital Euro' refers to the management of the ownership of euro amounts - similar to bank accounts - the 'digital, programmable euro' enables programmable payment processes. More specifically, using a digital, programmable euro payments can follow a certain logic and be executed automatically. These automatic processes already exist in the financial context, such as standing orders and interest payments. However, the digital, programmable euro enables significant efficiency gains, as even complex business processes can be implemented relatively easily via smart contracts. In contrast to non-DLT-based infrastructures the programmability of tokens becomes possible.

A single regulatory framework for digital tokens (crypto-asset) is currently under construction in the EU. In early 2018 the EC launched a research and consultation process to identify regulatory needs in this area, resulting in an action plan to create a single regulatory framework across Europe. This action plan is based on the following building blocks[21]:

- The adoption of non-legislative measures to provide guidance on how existing legislation should be applied to digital tokens;
- A pilot regime for DLT market infrastructures for digital tokens that qualify as financial instruments;
- A tailored regime for the issuance and operation of digital tokens not covered by financial services legislation.

There are numerous reasons for the introduction of a blockchain-based digital, programmable Euro. The main ones are the following: cross-border payments and integration with delivery vs. payment. Other reasons include: tokenizations of rights and assets, machine economy, IoT, micro payments and

[20] Prospect and Challenges of Cross-border Payment Posed by Digital Currency – From the Perspective of Blockchain Coalition, 2020, https://www.proquest.com/openview/f9f9f73715fe71e69f5223665afddea5/1?pq-origsite=gscholar&cbl=2040555

[21] Token Alliance, Legal Landscapes Governing Digital Tokens in the European Union, 2021, Legal-Landscapes-Governing-Digital-Tokens-in-the-European-Union.pdf

streaming money, IT security and system resilience. It is important to understand that existing systems may partly perform at least as well as blockchain systems in terms of some aspects (e.g., real-time payments).

Potential EU actions

In the current situation all token types entail different regulations and produce different requirements in regards to KYC, AML or regulation covering crypto-assets. The lack of a commonly accepted classification and taxonomy for blockchain technology and cryptographic tokens results in legal uncertainties for all stakeholders and therefore slows down the development of the technology and the adoption process.

A clear classification and taxonomy are needed to create legal certainty and avoid unexpected legal consequences or necessary design / technical changes after a system is built. With the proposal for the regulation on Markets in Crypto-assets (MiCA) presented by the European Commission on September 23, 2020, the first step in the right direction has been taken[22]. This proposal aims to harmonize regulation for crypto-assets and many related services in Europe. Despite current initiatives, further actions developing the regulatory framework is essential in order to support technology development. One of them is in place already: in October 2020 the European Central Bank (ECB) published the report on a digital euro. To date this report constitutes the most comprehensive analysis of the motives behind a European Central bank Digital Currency (CBDC) and its desirable characteristics[23].

For blockchains to live up to its full potential and avoid any system breaks, trusted payment tokens are crucial. Advantages range from higher resilience as single points of failures no longer exist and higher payment efficiency of real-time settlements. These tokens can be made programmable independent of the underlying system, thereby enabling automation for the industrial and financial sectors. While any kind of payment token could be used and would result in avoidance of unnecessary system breaks and assistance of real-time payments, the digital, programmable Euro would be beneficial in terms of default risk and would lead to higher acceptance and less friction in the long term and therefore could boost blockchain adoption. Policymakers should push for the implementation of a DLT-based digital programmable Euro.

Digital euro should comply with existing regulatory frameworks and Europe-wide regulations. Despite central bank liabilities being subject to regulation and oversight, the Eurosystem should strive to achieve compliance with existing regulatory standards, including those from the payments area[24].

[22] INATBA, Blockchain Ecosystem's Response to MiCA Regulation Proposal, 2021, https://inatba.org/wp-content/uploads/2021/03/2021-02-Blockchain-Ecosystems-Response-to-MiCA-Regulation-Proposal-Final.pdf

[23] EU Blockchain Observatory and Forum. Central Bank Digital Currencies and a Euro for the Future: https://www.eublockchainforum.eu/sites/default/files/reports/CBDC%20Report%20Final.pdf

[24] ibid

4. Additional input from stakeholders (insights from discussions)

As part of BlockStart activities, we aim to challenge the policy makers and regulators by inviting them to energizing discussions on the legislative and regulatory approaches concerning blockchain technology application and the challenges that come with it.

As identified and described in the previous section, there are 8 main challenges related to blockchain regulation. In our project context we have selected 2 different topics to explore further and discuss extensively during the webinars with industry experts.

Firstly, we have chosen DeFi regulation issues (as fintech is one of the most advanced sectors in terms of blockchain solutions). The emerging use of decentralized financial technologies may have implications for the effectiveness and enforceability of current regulatory frameworks, particularly when the current execution of supervisory activities focuses on the presence of centralized decision-making entities (e.g., financial intermediaries). The inability to regulate this new field might indeed slow down the pace of technological and business development. Therefore, given the need to better understand the challenges relating to DeFi regulation and its relevance, it was selected as a topic for the first webinar "Regulation of Decentralized Finance (DeFi)".

Secondly, a broader webinar topic for general discussion was selected, focusing on the regulation-caused barriers such as GDPR. Webinar "How to make sure regulation helps and not hinders blockchain development?" aimed to cover a broader context of regulatory impediments and limitations for blockchain development in both the public and the private sectors.

Detailed insights and recommendations obtained from the webinars are described below.

4.1 Discussion on regulation of decentralized finance (DeFi)

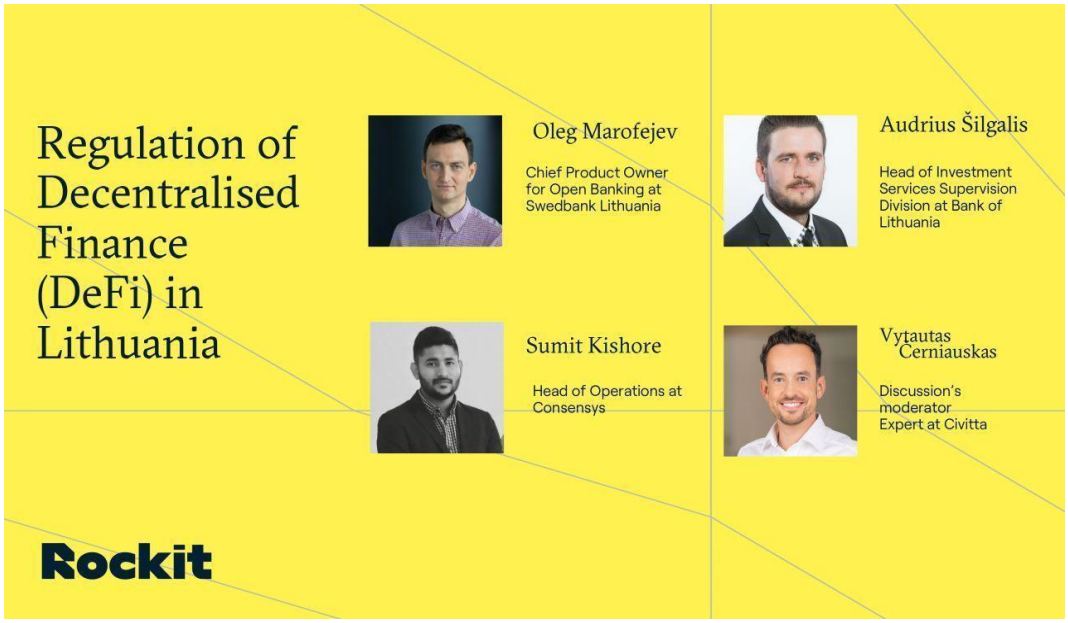
In order to collect feedback form key financial industry players, CIVITTA initiated a panel discussion "Regulation of Decentralized Finance (DeFi)." The event was co-organized with ROCKIT (https://www.rockitvilnius.com/), which is the prime space in Lithuania where top fintech innovators, creators and founders build the future of financial technologies. ROCKIT is a strong community featuring mentors, regular industry events and hosting acceleration programs. Joint forces of CIVITTA's expertise and ROCKIT community helped achieve higher engagement of ecosystem members.

The panel discussion took place on 12 November 2020 and was broadcasted live via Facebook (https://www.facebook.com/watch/live/?v=2731782303702519&ref=watch_permalink) and YouTube (https://www.youtube.com/watch?v=V3JzNJzTxFA). It was led by Vytautas Černiauskas, expert at CIVITTA, and included the following professionals:

- Audrius Šilgalis, Head of Investment Services of Bank of Lithuania,

- Oleg Marofejev, Chief Product Owner for Open Banking of Swedbank Lithuania, and
- Sumit Kishore, Head of Operations at Consensys.

Figure 3. The discussion panellists



The objective of the panel discussion was to articulate the emerging trends on the market, focusing on the relevant regulatory instruments that are already in place and areas where regulation is missing. The panelists were challenged to discuss regulatory and operational challenges in the DeFi realm as well as the improvements needed, and rethink whether the current framework that is in place to regulate the decentralized market needs to be re-assessed.

Discussion overview

The discussion started with the overview of the DeFi and how it is complementing and challenging the financial sector. Mr Oleg Marofejev of Swedbank, who has over 15 years of experience working in traditional bank focusing on digital development projects, gave his perspective on the main innovation trends arising from the technology and provided an overview of the actions and initiatives that traditional banks take in order to keep up with fast-paced technologies such as blockchain. According to Mr Marofejev, in order to remain up to date with the new trends, research and key studies are being conducted to fully understand the position of the traditional bank in the financial innovation world and how to act on certain changes to maintain competitive position.

Audrius Šilgalis of the Bank of Lithuania, the institution which is responsible for the development of a fintech-conducive regulatory and supervisory ecosystem, provided the background for the discussion by defining what financial innovation actually means. The Bank of Lithuanian representative has a strong background in financial innovation activities and is a member of Financial Innovation Standing Committee (FISC), also approaching 10 years of experience at Bank of Lithuania specialising in investment services supervision. Mr Šilgalis continued discussion by describing the main challenges facing the regulator and the need to balance the flow of innovation and ensure customer protection.

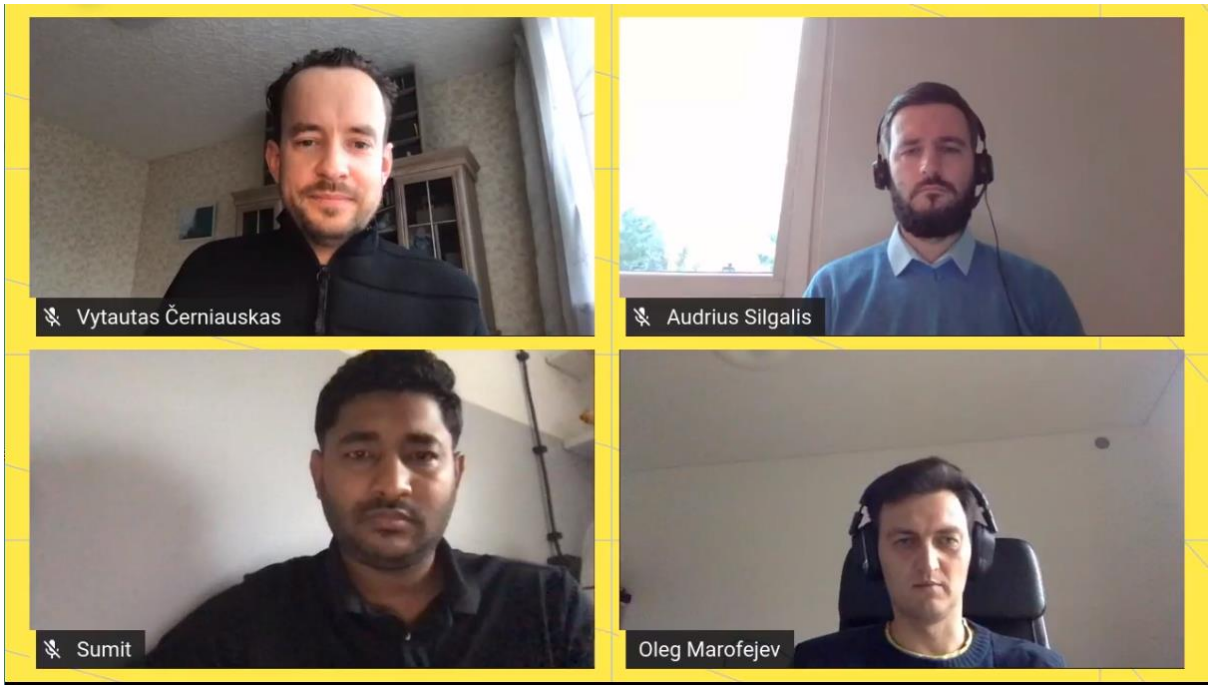
Mr Šilgalis noted that there is a lack of the central entity to explain the regulator requirements and singled out AML for having a lot of applicable regulation.

Startup ecosystem representative Sumit Kishore from Consensys, a blockchain solutions provider, highlighted the issues in DeFi and other similar innovations in the fintech area that innovators face from a regulatory point of view today, such as missing clarity on the regulatory framework that the companies have to follow. He also expressed the need for compliance tools that would help fulfil regulatory requirements. Mr Kishore, who is an active DeFi startup representative, keynote speaker in various international events, highlights his insights in compliance as his specialization.

In the discussion the need to ensure customer protection and avoid privacy breaches was highlighted. As well as the agreement that it is difficult or perhaps impossible to regulate a completely new and innovative field using old methods or approaches, and perhaps entirely new ways are needed.

The participation of a legislator, traditional financial institution and a blockchain innovator ensured a complementarity and inclusiveness of views, making sure that different regulator and innovators angles were presented.

Figure 4. Screenshot of the live event



Conclusions and insights

While the discussion touched upon a variety of many issues, the following key problems can be singled out:

- The current regulatory tools are not suited for many DeFi solutions.

- There is a strong need to ensure prevention of money laundering, financial crimes and financing of terrorism as well as having proper KYC procedures, the need to understand who you are working with.
- Ensuring security, consumer trust and consumer protection and protection of their data are key priorities of the regulation; the rights of customers need to be ensured so they can fully benefit from the DeFi solutions.
- Lack of central authority and regular interaction between the innovators and the regulators. Supervisors need to have contact with the DeFi companies to help them understand and implement regulatory requirements and who, on their end, can explain the solutions and logic behind the models they use.
- Lack of clearly defined regulatory framework and guidelines as the supervisory authorities are still learning and preparing regulation.
- From a regulation perspective, it is very difficult to understand how a regulator could apply regulatory powers and supervisory capability to a technology protocol that enables lending against assets without a lender (i.e., based almost entirely on an aggregate market value of assets mediated by way of a smart contract only).
- Other enquiries into the subject matter emphasize that a more decentralized financial system may reinforce the importance of an activity-based approach to regulation, particularly where it delivers financial services that are difficult to link to specific entities and/or jurisdictions. Certain technologies may also challenge the technology-neutral approach to regulation taken by some authorities.

Other inquiries into the regulation of DeFi also highlight the need to approach the risks in DeFi in newer ways.[25] The concerns that arise, when seeking to define the regulated activity and the regulated person, consider questions how to regulate against negative outcomes when there is no actual person responsible. This is going to require regulation on a more exclusive basis, for instance, responding to the risk of market harm to the consumers. This will present legislative challenges for the regulators unless they know the best practices of how to protect consumers.

Recommendations regarding DeFi regulation

In order to make the best use of the technology we need to either change the existing laws or create exceptions that address the specifics of DeFi.

DeFi companies can be regulated and provide safe and secure services to everyone. They should ensure due diligence, consumer protection and focus on good user experience (for example, what happens when users lose access to their wallets or are sharing their wallets). Many companies coming to the DeFi space are not completely aware of the regulatory framework they have to follow. There are already solutions available on the market that allow DeFi companies to meet the regulatory requirements and best practices and keep users safe and further education of such existing solutions is necessary.

[25] Regulation of Decentralised Finance (DeFi) in Europe, 2020, https://www.emergingpayments.org/article/regulation-of-decentralised-finance-defi-in-europe/

One way to go is to gradually apply to the DeFi industry the existing framework in a lighter perspective, which is already used to regulate the traditional centralized financial market players. While the traditional players complain of the heavy regulation and resources needed to ensure compliance, it ensures the protection of rights and interests of the service beneficiaries and other parties involved.

Another way is to implement regulation in a way different from the traditional method - to bring regulation from users, from the bottom up. The concept of decentralisation and the power of community could be used. There are enthusiasts who understand regulatory needs and could come up with either rules and regulations or define and structure problems. Maybe those central supervisory entities could have access to the general ledger and get information from there. When the problems are defined and specified by the community, regulatory experts from existing supervisory bodies could help in structuring solutions and then the technical community could implement them. This could be a much more efficient approach than the system currently used to regulate DeFi. Central authorities could also help in some unclear cases when specialty knowledge is needed.

The Bank of Lithuania was the first in Europe and one of the first in the World to create a blockchain sandbox for newcomer companies which want to develop and test blockchain-based solutions in a regulated market. This also helps the regulator to learn and understand what regulations could and should be applied to this kind of solutions. In general, the supervisory bodies need to think about new ways to regulate these innovations in crypto and blockchain space.

EC has presented new regulatory proposals of crypto assets (MiCA) to support innovation and to add consumer protection and a pilot regime for market infrastructures based on DLT. The purpose is to develop a secondary market for tokenized financial instruments and to encourage other innovations in this field. Market players and regulators should actively use existing consultation channels to provide their questions and suggestions to the EC in order to improve the proposals.

A strong recommendation for players creating innovative solutions is to not be afraid of regulators and talk to them directly explaining the models and concepts they are developing. In certain cases supervisory bodies could provide them with suggestions or recommendations and even help in making sure there are no legal grey areas. It is better to be regulated than to work outside the regulation and to be afraid of what happens if something goes wrong.

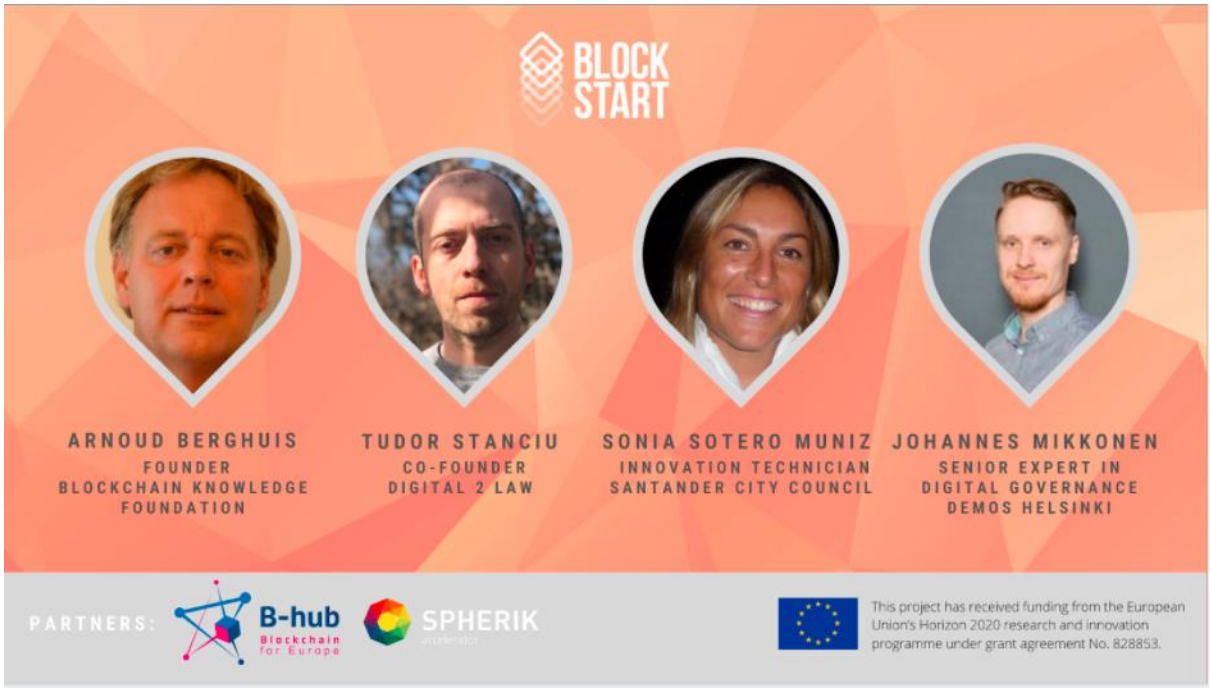
Figure 5. Post-event quotation shared on social media channels

4.2 Discussion "How to make sure regulation helps and not hinders blockchain development?"

The 2nd webinar "How to make sure regulation helps and not hinders blockchain development" was organized by CIVITTA and F6S, partnering with B-hub For Europe and Spheric Accelerator. The webinar as panel discussion took place on 27th of May 2021 and was broadcasted live via Facebook (https://www.facebook.com/events/615147312811822) and YouTube (https://www.youtube.com/watch?v=72se0K9C1zk&t=2s). The event was moderated by Vytautas Černiauskas, expert at CIVITTA, and included the following experts:

- Arnoud Berghuis, Dutch Blockchain Association and Blockchain Knowledge Foundation
- Tudor Stanciu, Co-founder of Digital2Law
- Sonia Sotero Muniz, New Technologies Department Manager at Santander Municipality
- Johannes Mikkonen, TOKEN project coordinator

Figure 6. Discussion panellists



Discussion overview

The discussion started with the overview of the BlockStart project and the regulation topic relevance in terms of efforts to foster blockchain technology development and massive adoption.

Mr. Stanciu gave a comprehensive presentation on blockchain technology from the regulation perspective, explaining main challenges, regulating principles and the GDPR effect on small and medium enterprises. One of the key elements of Tudor's presentation was the current and the foreseen Blockchain regulatory scenes.

Figure 7. Screenshot of the Mr. Tudor's presentation

According to Mr. Tudor, overall there is no single regulation on blockchain, rather there are certain areas where the EC plans to intervene to further their digital goals (agenda for Digital Europe) – initiatives typically revolve around dissemination of information and are still gathering data that will eventually lead to regulation – so far the only area of blockchain that made its way into law is in the field of crypto currencies (with MiCA and the Pilot Programme called the Pilot Regime Regulation for DLT Market Infrastructures (PRR)).

Another speaker – Arnoud Berghuis – introduced the concept of blockchain compliance by design, which means committing to the legal rules, policies and laws, handling the complex regulatory environment and if the technology is to be used for processing personal data, complementary mechanisms must be identified that provide support for building systems that meet security and data protection requirements.

Sonia Sotero Muniz, who presented the success story of Santander City Council and blockchain technology usage within governmental procedures and smart city projects, highlighted the regulatory challenges and obstacles they needed to overcome while working on a smart city project. Sonia agreed with the previously raised discussion about GDPR compliance, as it is one o fthe most important elements to comply with in order to succeed in those projects.

Key insights from Johannes Mikkonen presentation of regulation challenges reveal that there is danger of both – regulating too early or too late. There is a need to understand that blockchain can be implemented in any domain, but currently GDPR regulation isn't adjusted enough to seamlessly work in a decentralized scene.

In the discussion the compliance with GDPR topic was touched by all speakers, and it was highlighted as the key challenge for startups creating / developing blockchain-based solutions.

The participation of private and public sectors, representative of a legal background and a blockchain innovator ensured a complementarity and inclusiveness of views, making sure that different angles were presented.

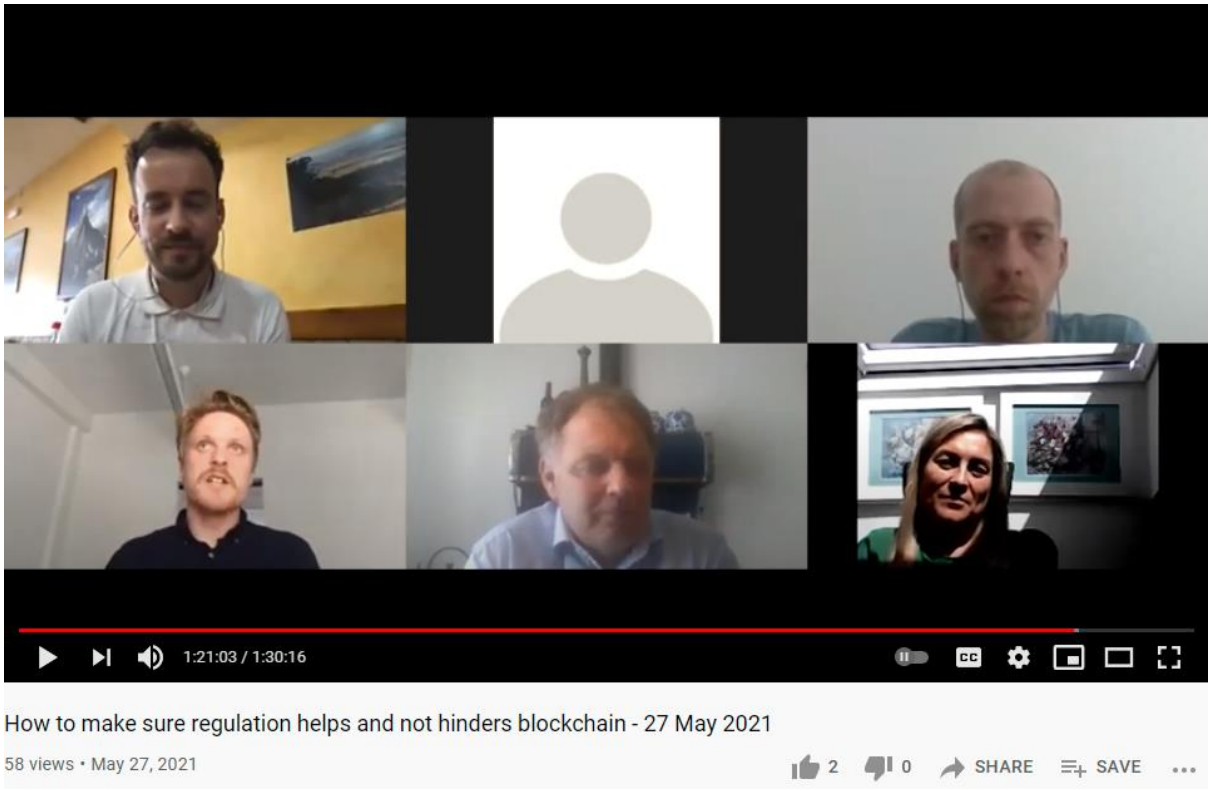
Policy recommendations obtained from the discussion

1. Johannes Mikkonen represented TOKEN (Transformative Impact of Blockchain Technologies in Public Services) project, which was launched in January 2020, an EU funded project whose ultimate goal is to develop an experimental ecosystem to enable the adoption of Distributed Ledger Technologies and to prove its value, via highly replicable use cases, as driver for the transformation of public services. According to Johannes, the governments shall set clear objectives and co-create together while developing regulatory framework. The cooperation would be easing the adoption of blockchain / DLT as drivers for more open, transparent, trusted and efficient businesses and public services.

2. Sonia Sotero Muniz from Santander City Council New technologies Department has experienced herself how current GDPR regulation affects technology development. According to Sonia, it is important to work all together and collaborate on regulatory framework creation so the needs and the requirements are corresponded accordingly. Regulatory guidance could indeed provide much legal certainty compared to the current status quo. This could take the form of various regulatory initiatives. On the one hand, regulators could coordinate through the European Data Protection Board (EDPB) to draft specific guidance on the application of the GDPR to blockchain technologies at a supranational level, thus avoiding the risk of fragmentation that would arise from numerous independent initiatives.

3. While blockchain technology is commonly considered potentially disruptive in various regards, there is a lack of understanding where and how blockchain technology is effectively applicable and where it has mentionable practical effects. This issue has given rise to critical voices that judge the technology as over-hyped and so slows down both the development of technology and the creation of a regulatory framework. Cross-domain collaboration is one of the key elements to consider while building an compliant ecosystem providing clear regulatory guidance.

Figure 8. Discussion screenshot from Youtube live session



5. Conclusions

Regulatory uncertainties over the formal status of blockchain applications are threatening and affecting the pace of the sustainable technology development for firms and other organisations either piloting blockchain or interested in its deployment and it can be considered as a high-risk business matter. The regulation is still developing and very few countries in the EU have set concrete rules to guide the Blockchain industry. Cyprus, Estonia, Malta and Switzerland are front-runners in this respect, but other regional laws or an EU-wide framework does not currently exist. So, it is very important to investigate various regulatory aspects in the field of blockchain / DLT and initiate further actions by providing some of the potential recommendations for policy makers.

Considering the current and future situation in terms of regulatory maturity, the financial sector is leading the way. The new Digital Finance package introduced by EC including Digital Finance and Retail Payments Strategies and legislative proposals on crypto-assets and digital resilience aim to provide a sound legal framework for all crypto assets not currently covered by the existing financial services legislation, thereby providing the necessary legal certainty required within the European Union for the development of the crypto-asset markets. The rudimental regulatory context of digital assets in finance is of utmost importance because this is blockchain's most developed area of use and so holds lessons for the technology's future regulatory aspects in other sectors as well.

Desk research suggests that the regulatory uncertainty could be break down into 8 challenges: Blockchain and GDPR; Standartization; Consumer and investor protection - identity management; Validity of smart contracts; Notary - legal recognition of signatures; Enforcement of anti-money laundering requirements; Applicable jurisdictions (including cross-border jurisdiction); Legal classification and taxonomy of tokens and digital programmable Euro. Research suggests that in some aforementioned challenges EU actions are quite significant. For instance, the already established and amended 5th anti-money laundering Directive (Directive (EU) 2018/843). On the other hand, there are other challenges that lack regulatory initiatives and concrete guidance. For example, it is unclear how storing personal data on blockchain exactly fits into the present regulatory environment. The immediate problem is that the precise meaning of data 'erasure' is left undefined which is conflicting with current GDRR principles.

The research supporting discussions revealed that one of the most common challenges which hinders development of blockchain-based solutions is GDPR, especially for the right to be forgotten (data erasure). Clarification on this matter is crucial in order to push the technology further.